(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/79972 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/40471

(22) International Filing Date: 9 April 2001 (09.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/551,098	18 April 2000 (18.04.2000)	US
09/602,218	23 June 2000 (23.06.2000)	US
09/602,219	23 June 2000 (23.06.2000)	US

(71) Applicant: **IOMEGA CORPORATION** [US/US]; 1821 West Iomega Way, Roy, UT 84067 (US).

(72) Inventors: **HALES, Ronald, F.**; 4052 S. 950 W., Riverdale, UT 84405 (US). **ISAACSON, Shawn, R.**; 4360 S. 2175 S., Roy, UT 84067 (US). **SHORT, Robert**; 7714 Crestview Drive, Niwot, CO 80501 (US). **PETERS, Eric**; 4099 W. 5600 S., Roy, UT 84067 (US). **ADAMS, Chad**; 5299 S. 2690 W., Roy, UT 84067 (US).

(74) Agent: **BUTTER, Gary, M.**; Baker Botts LLP, 30 Rockefeller Plaza, New York, NY 10112-0228 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

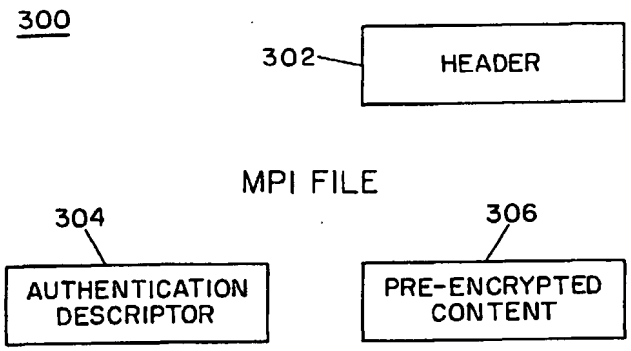
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR DELIVERY AND EXECUTION OF COPY PROTECTED DIGITAL CONTENT



(57) Abstract: A method and system are provided for first encrypting content with a first encryption key such as a random XOR key and then encrypting the first encryption key with a more complex, more difficult to decipher second encryption key which includes the unique ID code of the data storage medium receiving the content. One or more graphics, such as an advertisement or material associated with the content to be downloaded is provided with the file containing the content. The advertisement may be static or animated and is displayed at the time the content is played. Included in the file and associated with the graphic is a hyperlink such as an Internet hot link to an affiliated web site. Sponsors, which may include but are not limited to advertisers, content owners and content authors, can be charged for the initial view of a downloaded sponsor graphic on the web page, for associating the graphic and hyperlink to the file and/or for a percentage of payment for purchases made by traffic created by the hyperlink, among other charge options. After logging on to the host site, a registered client receives downloaded content merely by selecting the desired content, or merely by selecting the desired content and the desired download destination. An additional selection may be necessary if the content available for download is categorized, requiring a category selection followed by a content selection.

WO 01/79972 A2

METHOD AND SYSTEM FOR DELIVERY AND EXECUTION OF COPY PROTECTED DIGITAL CONTENT

SPECIFICATION

BACKGROUND OF THE INVENTION

The present invention relates to systems and methods for securely downloading copy-protected content over a network to users.

With the growth of digital compression, such as the MP3 standard, the distribution of audio and video content provided via the Internet is rapidly expanding. At present, it is estimated that hundreds of millions of illegal MP3 (music) files are downloaded from the Internet each month. Legal access to MP3 files via the Internet is problematic because of the ease in which the legally downloaded files can be copied and further distributed. As a result, owners of content are apprehensive of having their content distributed over the Internet because of the potential loss of revenue through unauthorized copying. Nonetheless, certain content may be legally available on the Internet either as promotional material or because the content owner has opted not to seek direct compensation from a user for the content provided. Audio and video content possibly can be provided in a format in which the downloaded content has limited playback capabilities. Alternatively, only a portion of the content may be provided, such as the first thirty seconds of a song. However, neither alternative is the optimum solution to consumers who may want to download complete content for their permanent use.

When content can be downloaded to a computer with no easy method of copying the content, a problem still remains in that the user, to best utilize the content, may need to have the content stored on a medium other than on the computer's fixed storage device, i.e., hard drive, or accessed from more that one type of device. Systems for discouraging and/or preventing unauthorized copying from removable media are disclosed in U.S. Patent Application Serial Nos. 09/061,493 filed April 17, 1998 to Kupka et al., 09/191,666 filed November 13, 1998 to Kupka et al., 09/191,676 filed November 13, 1998 to Kupka et al. and 09/191,989 filed November 13, 1998 to Kupka et al., which applications are commonly assigned to the

same assignee as the present application, the disclosures of each which are incorporated herein by reference.

Both content owners and consumers must endure and if possible resolve the problems associated with financial transactions, generally, and specifically financial transactions over the Internet. At the same time, companies have discovered benefits from advertising on the Internet. The benefit from the advertisement is understood to be increased by the number of times an advertisement is seen ("eyeballs"), or the amount of time an advertisement is displayed to the user ("stickiness"). Moreover, advertisers hope to maximize the number of people who see their advertisements, generally, and more specifically hope to maximize the number of people from their target audience viewing the advertisements. Storage media with pointers to remote network sites are disclosed in U.S. Patent Application Serial No. 09/519,772 filed March 7, 2000 to Tolson, which application is commonly assigned to the same assignee as the present application and the disclosure of which is incorporated herein by reference.

In addition, manufacturers and suppliers of hardware and data storage media in which content can be played and stored are seeking ways to increase sales and brand awareness. Other parties are seeking ways to obtain information through a network about consumers using the network.

Content providers and content owners are seeking ways to meet the security needs for copy-protecting downloaded content while at the same time reduce the time and computing power devoted to encrypting and decrypting the content. Further, content providers are seeking ways to generate traffic to other, both related and unrelated, websites. Finally, content providers are looking for ways to simplify the process for consumers to download content, thereby increasing usage by consumers.

SUMMARY OF THE INVENTION

Accordingly, it is an object of the present invention to provide a method and system for delivering content over a network which overcomes disadvantages in the prior art.

This and other objects of the invention are attained by providing a system and method for delivering content from a host site via a network to a client by having a host site receive a query from a computer of the client for the content selected by the client to be received by the client computer. The host site provides the selected content to a uniquely identifiable storage medium associated with the client computer, associating the received content with the uniquely identifiable storage medium such that the received content can only be accessed from the uniquely identifiable storage medium or alternatively, the uniquely identifiable storage medium is at least present in one of the disk drives in order for the client computer to access the content. The host site may further provide at least one advertisement to the client computer during at least one step of the method. In accordance with an aspect of the invention, the client is not charged a fee for the received content.

In accordance with an aspect of the invention, the client computer registers with the host site at least the first time the client computer communicates with the host site. The registration includes providing client software to the client computer for enabling the client computer to transmit information to the host site about the client computer and further including creating a random key or using existing unique identifiers in the client computer including but not limited to CPU and identification numbers, network identification numbers, network card identification numbers or additional hard drive information, to be stored on the client computer and providing the client computer with content player software for accessing the received content. The host site receives information about the client computer and/or the client from the client computer.

In accordance with another aspect of the invention, the content is stored to a uniquely identifiable removable storage medium. The content is encrypted using a unique code associated with the uniquely identifiable storage medium. If necessary, a unique code is generated, assigned and associated with the storage medium causing the storage medium to be uniquely identifiable.

In another aspect of the invention, a party compensates the content provider for information obtained by the host site via the client computer about the client or the client computer. In another aspect of the invention, the unique code is

permanently stored on the storage medium, cannot be copied to a second storage medium and is not accessible to the client.

In yet another aspect of the invention, the host site, prior to providing the selected content, determines the supplier of the uniquely identifiable storage medium and only provides the selected content when the supplier is recognized by the host site as a designated supplier of storage media.

In accordance with another aspect of the invention, a system is provided for delivering an advertisement to a client via a substantially blank storage medium containing the advertisement. The advertisement may include a hyperlink to a site on a communications network. The blank storage medium may further contain software for automatically displaying the advertisement when the blank storage medium is detected by a computer associated with the blank storage medium.

In accordance with another aspect of the invention, a content protection method and system is provided by first encrypting the content with a first encryption key such as a random XOR key and then encrypting the first encryption key with a more complex, more difficult to decipher (i.e. break) second encryption key which includes the unique ID code of the data storage medium receiving the content. The first encryption key is simpler, faster and requires less computing power than the second encryption key. Thus, once the encrypted first encryption key is decrypted at the client computer using the unique ID code of the data storage medium, the encrypted content can be quickly decrypted, thereby reducing the amount of time to download and decrypt the content received from the host site while still benefiting from the higher security level provided by the more rigorous second encryption key.

In accordance with another aspect of the invention, one or more graphics, such as an advertisement or material associated with the content to be downloaded is provided with the file containing the content. The advertisement may be static or animated and is displayed at the time the content is played. Included in the file and associated with the graphic is a hyperlink such as an Internet hot link to an affiliated web site. Because the graphic and hyperlink are attached to the file, a relationship between the file and the advertiser, content owner or content author is created for the life of the file. Sponsors, which may include but are not limited to

advertisers, content owners and content authors, can be charged for the initial view of a downloaded sponsor graphic on the web page, for associating the graphic and hyperlink to the file and/or for a percentage of payment for purchases made by traffic created by the hyperlink, among other charge options.

In another aspect of the invention, after logging on to the host site, a registered client receives downloaded content merely by selecting the desired content, or merely by selecting the desired content and the desired download destination. An additional selection may be necessary if the content available for download is categorized, requiring a category selection followed by a content selection.

BRIEF DESCRIPTION OF THE DRAWINGS

Further objects and advantages of the invention will be apparent from a reading of the following description in conjunction with the accompanying drawings in which:

FIG. 1 is a block diagram illustrating a system in which the method and system of the present invention can be employed;

FIG. 2 is a block diagram of various preferred embodiments of the present invention;

FIG. 3 is a flow chart showing certain aspects of the present invention of FIG. 2;

FIG. 4 is a flow chart showing further detail of block 116 of FIG. 3;

FIG. 5 is a flow chart showing further detail of block 140 of FIG. 4;

FIG. 6 is a flow chart showing further detail of block 166 of FIG. 3;

FIG. 7 is a flow chart showing further detail of block 192 of FIG. 3;

FIG. 8 is a front view of a computer monitor displaying a dedicated content player;

FIG. 9 is a flow chart of a method for use in conjunction with preferred embodiment of the present invention;

FIG. 10 is a flow chart of a preferred embodiment of the present invention;

FIG. 11 is a block diagram of a preferred embodiment of the present; invention;

FIG. 12 is a flow chart illustrating a preferred embodiment of the present invention;

FIG. 13 is a flow chart illustrating a further preferred embodiment of the present invention;

FIG. 14 is a diagram of a host site page of the invention shown in FIG. 12; and

FIG. 15 is a diagram of a second host site page of the invention shown in FIG. 12.

DESCRIPTION OF PREFERRED EMBODIMENTS

In a typical embodiment of the invention illustrated in the drawings, in Fig. 1, a client computer 20 is coupled via a communications network 22 to one or more remote network sites 24. The client computer 20 can be any of a number of devices including but not limited to personal computers, laptop computers, notebook computers, digital set-top boxes, satellite receivers, internet appliances or any other device that can receive content (not shown in Fig. 1) via a communications network 22. The client computer 20 typically is operated by a client 26, i.e., a user who desires to receive the content via the communications network 22. The content sought by the client 26 may include, but is not limited to, audio, video, text, games, animation, software and collectibles such as trading cards. More specifically, the content may include, but is not limited to, music, audio books, written materials such as books, magazines and lyrics, electronic text, photographs, movies, music videos, video games, statistics and data.

The communications network 22 can be any network over which the client computer 20 can communicate with one or more remote sites 24. The communications network 22 may include but is not limited to a wide area network (WAN), a local area network (LAN), an intranet or the Internet. Further, the communications network can include wireless access, call up access, fiber optic access, cable access and the like between the client computer 20 and remote sites 24. In an application where the communications network 22 is the Internet, the remote sites 24 are commonly know as web servers or web sites.

The client computer 20, interfaced with the communications network 22 such as the Internet, can function as a network client and receive information, typically digital information, from the web servers on the network. Application software on the client computer 20, such as conventional "browser" software 28 is typically adapted to request downloads from one or more of the servers in response to commands entered by the client 26.

The Internet is a worldwide computer network via which host computer systems communicate with one another using the well-defined Internet Protocol (IP). Typically, each host has a unique Internet address. To further define the addresses of resources on the Internet, the Universal Resource Locator system was created. A Universal Resource Locator (URL) is a descriptor that specifically defines a type of Internet resource and its location. The client 26, therefore, can access a web server simply by entering the server's URL.

In an Internet application, a network browser 28 running on the client data processing system typically includes programming for downloading content from the World Wide Web (the "Web"). The browser 28 is an operating system component or application program that allows the client 26 to retrieve content from the Web using any number of methods including simple point-and-click or voice enabled commands or the like. Typical browsers allow for multimedia presentation of content such as text, audio and video.

The client computer 20 can communicate with the remote sites 24 via the communications network 22 using any protocol defined for the network. For example, where the communications network 22 is the Internet, the client computer 20 and remote sites 24 can communicate with each other using well known protocols such as Internet Protocol (IP), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Hypertext Markup Language (HTML), Extended Markup Language (XML) or the like.

Preferably, the client computer 20 includes an internal or external storage drive 30 for storing and retrieving digital information, a central processing unit (CPU) 32 that controls the functions of the client computer 20, and a user interface (UI) 34 via which the client 26 can communicate with the client computer

20. The CPU can communicate with the drive 30 via a bus 36 by sending commands to write or read digital information to or from a data storage medium 38. The bus 36 can be any of the various buses, such as parallel, generic serial, USB, SCSI, and so on.

The data storage medium 38 can be any of the various data storage media including but not limited to magnetic, optical, magneto-optical or solid state. The data storage medium 38 can be fixed in the drive 30, or removable therefrom. Similarly, the drive 30 can be fixed in the client computer 20, or removable therefrom. Where the medium 38 is removable from the drive 30, the medium 38 can be encased in an outer shell 40 to protect the medium from damage. In an exemplary embodiment of the present invention, the data storage medium 38 is a removable medium such as optical (compact disk, DVD, CD-R, CD-RW, DVD-R, DVD-Ram, DVD-RW or the like), solid state (such as Compact Flash, Smart Media, Memory Stik® or the like), magnetic-optical or a nonvolatile, removable, magnetic medium, such as a magnetic disk, for use with a portable data storage drive. Examples of the latter include ZIP®, CLIK!™ or JAZ® drives (Iomega Corporation, Roy, Utah). Thus, the data storage medium 38 is coupled to the client computer 20. Such data storage medium in addition to being coupled to the client computer can also be stored on a network or on-line such as via the Internet.

The client computer 20 generally includes a user interface 34 with one or more input devices 42 and one or more output devices 44. For example, where the client computer 20 is a personal computer (PC), the input device 42 can include a mouse 42A and/or a keyboard 42B, and the output device 44 can be a monitor or video display terminal (VDT) 44A and can also include a speaker 44B. Similarly, where the client computer 20 is a digital set-top box (DSTB), the output device 44 can be a television screen, while the input device 42 can be a remote control unit.

Preferably, the data storage medium 38 has a plurality of data fields stored thereon, including a header field 46 and a content field 48. The content field 48 includes a representation, preferably a digital representation, of the audio or video content. Preferably, the header field 46 includes a substantially unique ID code that identifies the data storage medium 38. Preferably, the unique ID code is stored in the

medium 38 in a permanent, non-alterable fashion by the media manufacturer and as a person of ordinary skill would recognize may be part of a longer code. As used herein, the unique ID code refers to those where the statistical likelihood of duplication is reasonably low. For example, if psuedorandom assignment is used some, albeit minor, duplication may be encountered over large numbers of media. Preferably, the content in content field 48 is encrypted by an encryption method that incorporates or employs the unique ID code. The unique ID code can be a serial number, a random or pseudo-random sequence of alpha numeric or ASCII symbols or anything else that permits a computer, remote site or hardware device to distinguish among each individual data storage media of the same type as well as types of data storage media if necessary. Preferably, the unique ID code stored on the data storage medium 38 cannot be determined, copied or erased by the client 26.

Fig. 2 is a block diagram of an exemplary embodiment of the present system showing the interrelationships of the entities within the system. Portions of the system shown in Fig. 2 may be used separately without having to include the remainder of the system. The system will generally include one or more content providers 50, one or more content owners 52, one or more advertisers 54, one or more storage media and hardware suppliers 56 and one or more clients 26. The system may also include other parties 58 who receive information 59 such as usage, marketing, demographic or other similar type information related to (e.g., click-through traffic) or supplied by the client 26 on the client computer 20 to the content provider 50. The content provider 50 obtains permission, either directly or indirectly, from the content owner 52 to distribute content 60 to the clients 26, i.e., the users of the client computer 20, via a remote site 24 referred to as a host site 62 in Fig. 2. The host site 62, for example, can be a Web page of the content provider 50 on the Internet. The permission to distribute the content 60 may be tempered by restrictions, such as that the content provider 50 may only distribute the content 60 by a method that prevents unauthorized copying of the content once distributed by the content provider.

In consideration for the permission to distribute the content 60, the content owner 52 can receive many types of benefits from the content provider 50 or benefits from other parties 58. For example, a content owner 52 may receive

compensation directly from the advertiser 54, i.e., a company seeking to advertise its products or services through advertisements 64 during all or part of the preparation for or transmission of the content 60 to the client 26. The content owner 52 receives compensation directly from the advertiser 54 or via the content provider 50. The compensation may be structured any number of ways including but not limited to a fixed fee, a fee proportional to the number of times a potential client visits the host site 62 or a fee proportional to the number of times the same or different content 60 is delivered to clients 26. The content owner 52 may restrict the use of advertisements 64 placed prior to or during the downloading of the content owner's content 60.

The content provider 50, as stated above, typically arranges for advertisers 54 to advertise their products or services on the host site 62 for a fee. As with the content owners 52, the arrangements with the advertisers 54 can be structured in many ways. For example, the advertisements 64 may appear on the host site 62 prior to the client 26 selecting specific content 60 to be downloaded. Alternatively, the advertiser 64 may seek to have its advertisements 64 placed on the host site 62 only during the downloading of the content 60. The advertiser can also target advertisements 64 by having an advertisement appear only when certain content or types of content are or are not selected for downloading to the client 26. The system, thus, allows the advertiser 54 to target certain clients 26. As with the content owner 52, the cost of the advertisements 64 can be arranged in many ways, such as a fixed fee, a fee tied to client "hits" of the page containing the advertisement (i.e., the number of times the client is exposed to the advertisement) or the number of downloads of content 60 in which the advertisement was displayed. Alternatively, the content owner 52 and the advertiser 54 can negotiate directly for establishing the mechanism for the advertiser to compensate the content owner for permitting distribution of the content 60 in association with the advertisements 64 of the advertiser.

The content provider 50 can also enter into arrangements with suppliers 56 (including manufacturers) of data storage media 38 and hardware 65. For example, by agreement, the content provider 50 may restrict the downloading of content 60 to specific data storage media 38 provided by one supplier 56. The

compatibility of software or firmware for encryption and decryption of the content 60 may be limited to the data storage media 38 and hardware 65 of the supplier 56 who pay a fee to the content provider 50 to become an authorized supplier. As with the content owners 52 and advertisers 54, the compensation arrangement can be structured in many ways, including based on the number of downloads of content 60. Moreover, the content 60 may be downloaded in such a way that the hardware 65 capable of playback may be limited to suppliers 56 who have entered into an arrangement with the content provider 50. Further, the supplier 56 as part of the arrangement or possibly for an additional fee may display its trademarks and advertisements on the host site 62 as a branding partner of the content provider 50. Part of the arrangement between the supplier 56 and the content provider 50 can be that the data storage media 38 sold by the supplier, including "blank" data storage media, may contain advertisements for the host site and/or a hyperlink to the host site or even advertisements 64 or hyperlinks for the advertiser 54. Blank data storage media for purposes of this invention refers to storage media that are purchased or otherwise obtained by the user for their ability to store content as opposed to being purchased or otherwise obtained by the user solely for the content residing on the media at the time they are purchased or otherwise obtained. Preferably, an advertising blank storage media 67 contains software for displaying the advertisement to the user when the user accesses the blank storage media or automatically when the user's computer detects the blank storage media.

Fig. 3 is a block diagram of an exemplary embodiment of the method of the present invention. Starting at the top of Fig. 3 at functional block 100, the client 26 causes the client computer 20 to communicate with the host site 62 of the content provider 50. At block 102, once the client computer 20 establishes communications with the host site 62, the host site provides site information about the host site to the client 26, including but not limited to identification of the content 60 that can be provided, how the content is provided and any restrictions relating to the content being provided, such as the fact that content cannot be played back except on the data storage medium 38 from which it was first received from the host site. Along with the site information, the client 26 is provided with advertisements 64. At block

104, the host site 62 further requests certain initial login information from the client 26. Typically, such initial login information includes the client's name and email address. Optionally, the host site 62 may request a password so that clients 26 who are previous clients will be recognized by the host site.

Another alternative, shown at block 106, is for the host site 62 to check the client computer 20 automatically for cookies so that all or part of the login procedure can be bypassed. Cookies are information that reside on a computer such as the client computer 20 from a previous communication between the computer and a specific remote site such as the host site 62. For example, the information associated with the cookie when linked to a valid login name and password can provide the host site 62 with information required by the host site for download or information regarding client preferences pertaining to the downloading of content 60. At block 110, the host site 62 compares the cookie information and the client password information and, if necessary, the host site's stored database and if the cookie and password are associated, the host site bypasses the remaining login procedure at block 112 and the registration process at block 116. Additional information required for login may include but is not limited to the client's address and telephone number. In one embodiment, the host site 62 may verify the login information provided by the client.

In block 114, after the login information is accepted by the host site 62, the host site determines whether registration is required. The client 26 typically needs only to register the first time he or she seeks to obtain content 60 from the host site 62. The host site 62 determines whether registration is required by any number of ways including whether the client computer 20 already has the requisite software for receiving and decrypting content 60 originating from the host site 62. The host site 62 may also check whether a cookie for the host site resides on the client computer 20 or whether the client 26 provided an authentic password that matches the client's name.

Block 116 represents the registration process which is further described in Fig. 4. In one embodiment, advertisements are displayed to the client during all or part of the registration process. As shown in block 118 of Fig. 4 if registration is required, the host site 62 prompts the client 26 to register as a condition

of receiving content 60 from the content provider 50. The host site 62 also displays advertisements 64 to the client 26. In block 120 registration information 59 received by the host site 62 in block 118 is stored in a database associated with the host site. The information 59 requested during registration can vary greatly depending on the needs and desires of the content provider 50. The information 59 requested from the client 26 may include but is not limited to the email address and zip code if not already provided as part of the login process, the client's full mailing address and age. The content provider 50 can balance what information it would like to obtain with whether the registration process becomes too cumbersome that a client 26 does not complete the registration process. In an exemplary embodiment, in block 122, the host site 62, as part of the registration process, provides the client 26 with an agreement between the content provider 50 and the client in which the client in consideration for receiving the content 60 from the content provider grants permission to the content provider to download software onto the client computer 20, query the client computer for information 59. Such information 59 may include but is not limited to a computer identification number, the types of data storage media 38 and drives 30 associated with the client computer, the geographic location of the computer, a pre-existing unique ID code (i.e., serial or identification number) associated with any data storage medium 38 detected by the host site 62, and the capacity remaining on the data storage medium detected by the host site. The agreement may also seek permission to provide all or a portion of the information 59 obtained by the host site 62 to other parties 58. The agreement may further require the client 26 not to attempt unauthorized distribution of content 60 received from the host site 62.

Acceptance of the agreement can be requested by the content provider 50 at any time during the registration process. As shown in block 124, the client 26 typically would be required to accept or decline the agreement before proceeding further. If the client 26 declines the agreement, the host site 62 can inform the client that it will be unable to provide the content 60 to the client or alternatively, as shown in block 126, the host site could break down the parts of the agreement and query the client 26 as to which terms the client will not agree and depending on the response in

block 128, may permit or not permit the client to receive content as shown in block 130. In block 132 the client 26 is informed if the host site 62 does not accept the client's response. If the host site 62 accepts the agreement, registration continues in block 134. During registration as shown in block 134, the host site 62 can also query the client 26 as to whether to permit a cookie to reside on the client computer 20 to streamline the login and downloading procedures during subsequent visits to the host site. If yes, in block 136 the cookie is retained on the client computer 20 and if no, in block 138 the cookie is deleted from the client computer 20.

In block 140, as part of the registration process, the host site 62 downloads software to the client computer 20. The software downloading process provides another opportunity for the host site 62 to display advertisements 64 to the client 26. In a typical embodiment, two types of software are downloaded; however they can be combined into one software application. The first is a client software application which permits the host site 62 to obtain information 59 from the client computer 20 each time the client computer logs in to the host site. The information 59 may include but is not limited to determining (1) the types of drives associated with the client computer, (2) unique ID codes from data storage media 38 it detects and recognizes, and (3) data storage media usage information. Additional exemplary functions of block 140 are further shown in Fig. 5.

Referring to Fig. 5, in block 141 the client software is downloaded and in block 142 a random key is created and stored in the client computer 20 such as on the hard drive or other storage unit. A person of ordinary skill in the art would understand that keys other than random keys can be used as described hereinabove. The random key is used for encrypting and decrypting the content 60. In block 144 the client software includes a prompt for providing a default destination for the content 60 to be received. If the client 26 desires a default destination, it is installed at block 146. In block 148, an autoexecute function is offered as part of the client software for initiating automatic play back of content 60 if the client computer 20 recognizes a removable data storage medium 38 containing content 60 obtained from the host site 62. It is either accepted by the client 26 and thus installed as shown in block 150 or if declined, the client in block 152 is asked if he or she desires the client

computer 20 to prompt the client as to whether he or she wants to play back the content 60 residing on the installed removable data storage medium when one is detected. If yes, that software is installed on the client computer 20 at block 154.

In block 158, the second set of software, a content player software application 310, is downloaded by the host site 62 to the client computer 20 during registration. The content player software uses the downloaded random key and the unique ID code associated with the data storage medium 38 that contains the content 60 to decrypt the content on the data storage medium at the time of playback. At this point, as shown in block 160, the registration software download is completed. Registration is now complete. As the two types of software, client software and content player software, can be combined, subsequent reference to content player software 310 includes the client software.

At block 161 of Fig. 3, the client 26 and/or the client computer 20 provide or update the host site 62 with the information 59. Next, in block 162, the host site 62 prompts the client 26 to select the content 60 to be received. In an exemplary embodiment, the content 60 to be received is music and the host site 62 provides a database listing of the content available arranged in any of a number of ways, including but not limited to alphabetical by artist, song, album or musical category, such as country, rock or classical. The host site 62 may also provide database search capabilities to assist the client 26 in finding the content 60 desired. In block 164, the client 26 selects the music to be downloaded. In block 166, the host site 62 determines the destination for downloading the content 60.

Fig. 6 shows in more detail the method for determining the destination for downloading of software in block 166. At block 168 of Fig. 6, the host site 62 searches for a default drive, i.e., the host site requests the default drive from the client computer 20. In block 170 the host site 62 determines if the default drive was found. If yes, in block 172, the host site 62 prompts the client 26 to decide if the client wants to download content to the default drive. If yes, in block 174 the download is set for the default drive. If the default drive is not found, in block 176, the host site 62 queries the client 26 as to where the content should be downloaded. In block 178, the

client 26 selects the location and in block 180 the host site 62 sets the download for the selected location.

Returning to Fig. 3 from block 181, in block 182, the host site 62 determines if the data storage medium 38 residing in the drive 30 of the client computer 20 selected to receive the content 60 is acceptable to the host site for downloading content. If it is not acceptable, at block 184 the host site 62 informs the client 26 why the download cannot proceed and provides the client with the option to correct the problem at block 186. If the problem is corrected, at block 188, the client 26 is returned to block 166, determining download destination. If the problem is not corrected, at block 190, the host site 62 can return to the initial display at block 102.

Returning to block 182, if the selected media is acceptable, the host site 62 determines in block 192 whether the data storage medium 38 has or can have a unique ID code. In an exemplary embodiment, the data storage medium 38 is a removable data storage medium such as a ZIP® or CLIK!™ or JAZ® (Iomega Corporation, Roy, Utah) or the like. These removable storage media are protected by any proprietary technique that is based on unique serial numbers that cannot be erased, copied or easily determined by the client 26.

Fig. 7 further details the process of block 192, starting at block 194, where it is determined whether the storage medium 38 has a unique ID code. If yes, the process continues from block 192. In block 198 if the storage media 38 does not have a unique ID code and it is determined in block 190 that one can be assigned that cannot be copied or determined by the client and preferably cannot be erased, the host site 62 in block 200 creates and assigns or obtains the substantially unique ID code. If the unique ID code cannot be assigned, in block 202 the process returns to block 184 where the client 26 is informed that the content 60 cannot be downloaded to that media. Alternatively, the host site 62 can be programmed not to permit transfer of content 60 to removable storage media, or even a hard drive, that does not have a pre-existing unique ID code that cannot be erased, copied or determined by the client 26. As stated above, the content provider 50 may limit the downloading of content 60 to specific data storage media, such as to the data storage media of the supplier 56.

Returning to Fig. 3, once the unique ID code is determined, the host site 62 in block 204 encrypts the content using the random key associated with the client computer 20. The random key uses the unique ID code in encrypting the content 60. In block 206, the encrypted content 60 is then downloaded to the data storage medium 38 previously selected by the client 26.

Throughout the time that the client 26 is viewing the host site 62, the host site can display advertisements 64 of the advertisers 54. The advertisements 64 can take many forms including visual, video, audio, static or dynamic animation, or any combination thereof. Branding for purposes of this invention, can be a form of advertisements 64. Certain points in the process of the client 26 receiving the content 60 provide unique opportunities for maximizing the value of the advertisements 64. For example, during registration in block 116, audio advertisements may be preferred. During periods in blocks 141 and 158 in which client software and content player software are being downloaded, video or dynamic animation may be preferred. During periods of downloading, the advertisement 64 can be integrated with an indicator of the progress of downloading. Typically, a computer visually indicates the progress of downloading or copying information to the data storage media 38 of the computer. It may be as simple as a succession of boxes being filled in from left to right or a percent completion may be indicated numerically. In an embodiment of the invention, in addition to or in lieu of the standard indicator of completion, an indicator can be used that incorporates an advertiser's product or service. For example, if the content 60 being downloaded includes baseball cards or data, the indicator may show a baseball progressing from being hit to reaching the fences with the position of the ball relative to the batter and the fence providing an indication of the percent completion of the download. The advertiser 54 for this display may, for example, be a baseball league. The length of time that may be required for downloading large content, such as books, movies or music albums, may provide the opportunity for video advertisements.

Moreover, advertisements 64 could be embedded in the encrypted content such that advertisements could be displayed before, during or after each playback, including the possibility of having the advertisements 64 change over a

period of time or after a number of plays. The advertisements 64 could be in the form of "skins", which are software applications that provide the look of the "player" or something else during playback. For example, when music is played using the compact disk drive of a computer, the computer monitor display 66 often provides a representation of a compact disk player 68 as shown in Fig. 8. The content 60 can be encrypted such that when the music is played back, the computer monitor display 66 takes on a look that incorporates advertising or, more specifically, branding information. Alternatively, the skin could be associated directly with the content 60. For example, when the content 60 is played back, in this instance a song, a picture of the artist or of an album cover can be integrated into the skin.

In block 210 after the content 60 is downloaded to the data storage media 38 associated with the client computer 20, the host site 62 may prompt the client 26 to determine if additional content is desired. In one embodiment, the host site 62 may only allow, for example, one song to be downloaded at a time so that the client 26 may have to separately download each song on an album. Such an embodiment would increase the number of times that the client 26 is exposed to the advertisements 64 associated with the host site 62 or more specifically, the content owner 52. If no other content 60 is requested, the client 26 at block 212 can return to the initial display of the host site at block 102 or can leave the host site.

Fig. 9 shows the steps of playing back the content 60. In block 214, whenever the client 26 desires to play back the content 60 using the client computer 20, the client 26 selects the content player software already installed on the client computer. In block 216, the client computer 20 searches for the software. If it is not found, in block 218, the client 26 is informed of the problem. If the player software is found, in block 220 the content player software searches for the content 60 associated with the host site 62 to determine the correct drive for the stored content. If the software cannot determine the location of the content 60, the client 26 is prompted in block 222 to supply the source drive or folder and possibly select the content 60 to be played back. Once the content 60 is located, in block 224 the content player software searches for the unique ID code of the media which has been cryptographically associated with the content 60. If the unique ID code is not found, in block 218 the

client is informed of the problem. If the unique ID code is found, in block 226 the content player software decrypts the content 60 using the random key associated with the client computer 20 and the unique ID code associated with the data storage medium 38 containing the content. In block 228, the client computer 20 plays back the content 60 and, if applicable, displays an advertisement.

In situations where the data storage medium 38 is a removable data storage medium such as a ZIP® disk, the removable storage media containing the content 60 to be played back can be inserted into any appropriate drive designed to receive the removable data storage medium. The drive 30 may be associated with another computer (i.e., a computer other than the client computer 20) or may be associated with a dedicated playback hardware device such as a compact disk player or an MP3 player. If the hardware or computer associated with the removable storage medium 38 has content player software or firmware, the content 60 is decrypted and played as described above. If the hardware or computer does not have the content player software, it can be downloaded from the host site 62 or can be copied from the hard drive of the client computer 20. In an alternative embodiment, the content player application software can be downloaded directly from the host site 62 to the removable data storage medium containing the content 60, with autoexecuting software either to automatically install the content player software to any computer in which the removable data storage media is read, or at least to prompt the computer user to install the content player software.

The method and system for delivering content 60 meets the needs of content owners 52, clients 26, advertisers 54, content providers 50 and data storage media and hardware suppliers 56. Content owners 52 receive the fees for their work from the advertisers 54. The possibility of unauthorized distribution is minimized first because unauthorized decrypting of the content 60 is difficult and second because there is no advantage for a person attempting unauthorized decryption because that person can just as easily obtain the content for free from the content provider's host site 62. Further, the content owner 52 has the option of licensing the content 60 directly with the content provider 50 or the advertiser 54 and can negotiate terms in any number of ways including a flat fee, per site visit, per download of content,

among others. The client 26 benefits by obtaining a permanent copy of the content 60 for free. Moreover, by using a removable storage medium, the client 26 can playback the content 60 on any content player that can read the data storage medium 38. The client 26 also receives the ancillary benefit of better storage media 38 and hardware 65 as a result of providing the manufacturer and supplier 56 of these products with information 59 they can use to provide the client 26 with better products. Advertisers 54 benefit because they receive exposure of their advertisements 64, possibly for extended periods of time, not only to a large audience, but also to a targeted audience. The content provider 50 benefits either by receiving a percentage of the fees paid by the advertiser 54 or as a result of the exposure of the content provider to the target audience and the good will created by having a host site 62 that delivers free content 60 to clients 26.

The manufacturer and supplier 56 of the data storage media 38, especially the removable storage media, and the hardware 65 used to play back the content 60 benefit through increased sales of their products. Moreover, the manufacturer and supplier 56 of the storage media 38 and hardware 65 also benefit from the information 59 obtained from the client 26 and the client computer 20 regarding the use of the storage media 38 and hardware 65. Other parties 58 benefit, who obtain the information 59 the client 26 agrees to provide.

The content provider 50 further may also be the content owner 52, the supplier 56, the advertiser 54 or another party 58 and thus reaps the benefits ascribed above to these entities. Any of the above entities may further benefit from the method and system of the invention by taking on the role of another entity. For example, the supplier 56 of the removable storage media may also be the content provider 50. The supplier 56 may also be an advertiser 54. The content owner 52 may opt to be the content provider 50 and also advertise on the host site 62. In other words, each of the content owner 52, the supplier 56, the advertiser 54 or an information seeking party 58 can run the host site 62.

Fig. 10 shows the method for providing an advertisement on a blank storage medium to a user. The advertisement may be a sample of content, such as a song from an album. In block 232, an advertisement is obtained by the supplier of the

blank storage medium, which could include the manufacturer. In block 234, the blank storage medium is obtained. In block 236, the advertisement is loaded onto the blank storage medium. Alternatively, a hyperlink to a site on the communications network 22 at block 238. In block 240, software can be loaded onto the blank storage medium for accessing the advertisement by a computer associated with the storage medium. In block 242, software for automatically accessing the advertisement when the computer detects the blank storage medium can be installed. Finally, in block 244, the blank storage medium with the advertisement is provided to the user.

Fig. 11 shows a preferred encrypted file format for downloading and playing content 60, such as music, using a content player. Other embodiments are contemplated by this specification as will be understood by those skilled in the art, such as using different file structures. Fig.12 shows a preferred content encryption and delivery method. The layout for encrypted files disclosed herein, which will be referred to as MPI files 300, can, for example, be used with a content player such as the client computer 20 or a dedicated hardware device or a software player such as the Iomega ZAmp$^{3™}$ player (Iomega Corp., Roy, Utah), among others. MPI files include a header 302, an authentication descriptor 304 and pre-encrypted content 306. In this embodiment, the pre-encrypted content 306 is MP3 formatted music. MPI files 300 provide secure transfer of content 60 from the host site 62 of the content provider 50 to the data storage medium 38 of the client 26. MPI files 300 also tie the content 60 directly to the data storage medium 38. The playing of MPI files 300 and display of the associated graphic and hyperlink on the player create recurring Internet traffic and sales revenue for content providers 50, content owners 52 and advertisers 54, among others. In a preferred embodiment, the associated graphic is the advertisement 64.

The pre-encrypted content 306 is encrypted using an XOR file key which is a 64-bit XOR encryption algorithm. There is no padding space between these elements. Blowfish encryption is then used to encrypt the XOR file key. However, any encryption standard could be used. The Blowfish algorithm is a variable-length key, 64-bit block cipher and is available for download via http://www.counterpane.com/blowfish.html (Counterpane Internet Security, Inc., San Jose, California). The Blowfish algorithm consists of two parts: a key-expansion part

and a data-encryption part. The key expansion part converts a key of at most 448 bits into several sub key arrays totaling 4168. Data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation and a data-dependent substitution. All operations are XORs (i.e., exclusive or) and additions on 32-bit words. The only additional operations are four indexed array data lookups per round. The Blowfish algorithm uses the unique ID code, in this embodiment a 40 byte unique ID code, of the data storage medium 38 in creating the Blowfish encryption key.

The terms used in the encryption method are defined in Table I. All four byte numerical values represent an unsigned 32-bit number. All two byte numerical values represent an unsigned 16-bit number.

Table I - Definitions

Type	Description
BP	Byte Pointer
BYTE	A string of 8 binary digits operated upon as a unit
WORD	A string of 16 binary digits operated upon as a unit
LONG	A string of signed 32 binary digits operated upon as a unit
ULONG	A string of unsigned 32 binary digits operated upon a unit
User-PC Application	An Application installed to a user's PC or other hardware that makes use of MPI files.
Header Byte Order	Little-Endian (Intel format MSB/LSB)

As shown in Table II, the header 302 provides information to determine the content and size of the authentication descriptor 304.

Table II – Header

BP	Field name	Content
1 to 2	File Version Information (High)	Numerical value
3 to 4	File Version (Low)	Numerical value
5 to 8	Authentication Descriptor Length (LEN_AUTH)	Numerical value

The file version information field specifies two 16-bit numbers that represent the version range of the MPI file 300. This allows the content player,

including but not limited to the client computer 20 or dedicated playback hardware devices, the ability to handle legacy MPI files if the authentication descriptor 304 changes in the future. The high value is the upper version range and the low value is the lower version range that the content player supports. The authentication descriptor length field specifies a 32-bit number that represents the length, in bytes, of the authentication descriptor 304. This value should not be zero.

The authentication descriptor 304 is a non-encrypted structure that contains information about the pre-encrypted content 306. This descriptor 304 contains two field values (i.e. authentication string and XOR file key) that are encrypted using the Blowfish algorithm. Thus, once the authentication descriptor 304 is read in, the two field values (i.e. authentication string and XOR file key) can only be decrypted using the Blowfish algorithm which incorporates the unique ID code. The fields of the authentication descriptor 304 are listed in Table III.

Table III – Authentication descriptor

Byte Position	Field name	Content
9 to 9	OS type	Byte
10 to 10	Device type	Byte
11 to 11	File type	Byte
12 to 12	Encryption/Encode Type	Byte
13 to 20	MPI authentication string	Character bytes
21 to 28	MPI "XOR" file key	Character bytes
29 to 32	Embedded GIF/AVI length (LEN_GRPH)	Long
33 to 34	Embedded URL_1 length (LEN_URL1)	Word
35 to 36	Embedded URL_2 length (LEN_URL2)	Word
37 to 38	Embedded ID3 Tag length (LEN_ID3 Tag)	Word
39 to (39+LEN_ GRPH)-1	Embedded GIF/AVI (Content body)	Character bytes
(39+LEN_ GRPH) to (39+LEN_GRPH+LE N_URL1)-1	Embedded URL_1 (Graphic URL)	Character bytes
(39+LEN_GRPH+LE N_URL1) to(39+LEN_GRPH+L	Embedded URL_2 (Artist URL)	Character bytes

EN_URL1+LEN_URL 2)-1		
39+LEN_GRPH+LEN _URL1+LEN_URL2) to (39+LEN_GRPH+LE N_URL1+LEN_URL2 +LEN_ ID3TAG)-1	Embedded ID3 Tag	Character bytes

The operating system (OS) type field contains an 8-bit byte that describes the operating system type of the MPI file 300. A download server software application 312 associated with a download server associated with the host site 62 of the content provider 50 sets these bits prior to downloading content 60 to the client 26. The following OS Types are typically used:

0 = WIN32

1 = MAC

The device type field contains an 8-bit byte that describes the device type. The content player uses the device type bits to determine from what device and thus data storage medium 38 to query for the unique ID code incorporated in the Blowfish encryption key in order to unlock the Blowfish-encrypted authentication string and XOR file key stored in the authentication descriptor 304. The download server software 312 sets these bits prior to downloading content 60, in this instance music, to the client 26. The following device types are typically used:

0= removable type (e.g. Iomega removable type)

1= hard drive type

2= CD type

3= other type (e.g. flash memory, etc...)

The file type field contains an 8-bit byte that describes the file type. The content player uses the file type bits to determine what type of internal bitmap skin to use on the player when playing music. The download server software 312 sets these bits prior to downloading music to the client 26. The file types typically are:

0= Normal audio (MP3/MPI)

1= Audio books

The encryption/encode type field contains an 8-bit byte that describes the encryption/encode type applied to the audio body portion of the MPI file. The encryption/encode type is typically 0=XOR Encryption.

The authentication string field contains the authentication string. The authentication string is used to validate the MPI authentication descriptor. This string is loaded by the download server software 312 prior to download to the client 26 and is encrypted with the Blowfish algorithm using the unique ID code of the data storage medium 38 as the Blowfish encryption key.

The XOR file key field contains the Blowfish-encrypted XOR file key. The random 64-bit (8-Byte) XOR file key is pre-determined by the download server software 312. The unencrypted XOR file key is applied to the MP3 file content prior to download of the MP3 file content to the client 26. The XOR file key is also encrypted with the Blowfish algorithm using the unique ID code of the data storage medium 38. The content player will first decrypt the Blowfish-encrypted XOR file key stored in the authentication header using the unique ID code of the data storage medium 38 and then will use the decrypted XOR file key to decrypt the pre-encrypted MP3 file content.

The length of embedded GIF/AVI content field specifies, as a 32-bit number, the length in bytes of the embedded GIF/AVI advertising content file containing the advertisement 64. The length of the GIF/AVI content field can vary as necessary to support the application. The length of embedded URL hyperlink 1 field specifies, as a 16-bit number, the length in bytes of the embedded URL hyperlink associated with the advertisement 64. The length of embedded URL hyperlink 2 field specifies, as a 16-bit number, the length in bytes of the embedded URL hyperlink associated with the artist/source of the content 60, in this embodiment, music. The length of embedded ID3 Tag field specifies, as a 16-bit number, the length in bytes of the embedded ID3 Tag.

The embedded GIF/AVI content contains the embedded advertising graphic content. The graphic is pre-selected from a database of advertising content on

the download server and is embedded in the MPI authentication descriptor prior to downloading to the client 26. The file can contain animated frames and/or a static frame. The graphic can also be in JPEG, BMP, PNA, MNA, ASF, WMA or MPEG format or the like.

The embedded URL hyperlink 1 field contains the embedded graphic content URL hyperlink. The embedded URL hyperlink 1 will be selected from a database of advertising content on the download server. The embedded URL hyperlink 1 will most likely be associated to the embedded advertisement 64 and is embedded in the MPI authentication descriptor 304 prior to downloading to client 26.

The embedded URL hyperlink 2 field contains the embedded artist URL hyperlink. The embedded artist hyperlink is associated with the artist/source of the MPI file audio content.

The embedded ID3 tag field contains the embedded ID3 Tag information. The ID3 Tag, one part of the MPI format, provides a flexible way of storing information relating to an audio file within itself to determine its origin and contents. The ID3 Tag information is stored in the last 128 bytes of an MP3 file if the ID3 Tag exists. The string-fields will contain NULL terminated ASCII-data. The format of the ID3 Tag is provided in Table IV. An album track number can be added to byte position 29 in the Comment field. Table V provides the genre codes and descriptions.

Table IV – ID3 Tag Description

Field	Description	Length (bytes)	Offset
TAG	Field = "TAG" if ID3 Tag is valid	3	0-2
Title	Title of MPI file	30	3-32
Artist	Artist of MPI file	30	33-62
Album	Album where MPI comes from	30	63-92
Year	Year when song was released	4	93-96
Comment	Comment field for MPI File	29	97-125
AT	Track number of Album	1	126
GE	Genre field (e.g. Table-III)	1	127

Table V – Genre Description

GE Code	Description	GE Code	Description	GE Code	Description
00	Blues	49	Gothic	98	Easy Listening
01	Classic Rock	50	Darkwave	99	Acoustic
02	Country	51	Techno Industrial	100	Humour
03	Dance	52	Electronic	101	Speech
04	Disco	53	Pop Folk	102	Chanson
05	Funk	54	Eurodance	103	Opera
06	Grunge	55	Dream	104	Chamber Music
07	Hip Hop	56	Southern Rock	105	Sonata
08	Jazz	57	Comedy	106	Symphony
09	Metal	58	Cult	107	Booty Bass
10	New Age	59	Gangsta	108	Primus
11	Oldies	60	Top 40	109	Porn Groove
12	Other	61	Christian Rap	110	Satire
13	Pop	62	Pop/Funk	111	Slow Jam
14	R&B	63	Jungle	112	Club
15	Rap	64	Native US	113	Tango
16	Reggae	65	Cabaret	114	Samba
17	Rock	66	New Wave	115	Folklore
18	Techno	67	Psychadelic	116	Ballad
19	Industrial	68	Rave	117	Power Ballad
20	Alternative	69	Showtunes	118	Rhythmic Soul
21	Ska	70	Trailer	119	Freestyle
22	Death Metal	71	Lo Fi	120	Duet
23	Pranks	72	Tribal	121	Punk Rock
24	Soundtrack	73	Acid Punk	122	Drum Solo
25	Euro Techno	74	Acid Jazz	123	Acapella
26	Ambient	75	Polka	124	Euro House
27	Trip Hop	76	Retro	125	Dance Hall
28	Vocal	77	Musical	126	Goa
29	Jazz+Funk	78	Rock & Roll	127	Drum & Bass
30	Fusion	79	Hard Rock	128	Club House

31	Trance	80	Folk	129	Hardcore
32	Classical	81	Folk Rock	130	Terror
33	Instrumental	82	National Folk	131	Indie
34	Acid	83	Swing	132	BritPop
35	House	84	Fast Fusion	133	Negerpunk
36	Game	85	Bebob	134	Polsk Punk
37	Sound Clip	86	Latin	135	Beat
38	Gospel	87	Revival	136	Christian Gangsta Rap
39	Noise	88	Celtic	137	Heavy Metal
40	Alternative Rock	89	Bluegrass	138	Black Metal
41	Bass	90	Avant-garde	139	Crossover
42	Soul	91	Gothic Rock	140	Contemporary Christian
43	Punk	92	Progressive Rock	141	Christian Rock
44	Space	93	Psychedelic Rock	142	Merengue
45	Meditative	94	Symphonic Rock	143	Salsa
46	Instrumental Pop	95	Slow Rock	144	Trash Metal
47	Instrumental Rock	96	Big Band		
48	Ethnic	97	Chorus		

An MPI file name is created using the artist/title information from an ID3 Tag, which is typically appended to most MP3 files. The content player defaults to using the file name of the MPI file in order to identify the artist's title information if no ID 3 Tag is provided in the authentication descriptor (e.g. Artist-Title.MPI).

An example of a header description in 'C/C++' language is as follows:

```
// Header Descriptor
typedef struct
{
    WORD        ulFileVersionHigh;
```

```
        WORD        ulFileVersionLow;
        ULONG       ulAuthenticationLen;
    }MPI_HeaderDescriptor

    // Authentication Descriptor
    typedef struct
    {
        BYTE        cOSType;
        BYTE        cDeviceType;
        BYTE        cFileType;
        BYTE        cEncyrption/EncodeType;
        BYTE        szMPIAuthenticationStr[8];
        BYTE        szXORFileKey[8];
        ULONG       ulGifGraphicLen;
        WORD        wURLHyperLinkLen1;
        WORD        wURLHyperLinkLen2;
        WORD        wID3TagLen;
        // Embedded Gif/AVI body goes here
        // Embedded URL1 Hyperlink goes here (Content URL)
        // Embedded URL2 Hyperlink goes here (Artist URL)
        // Embedded ID3 Tag body goes here
    }MPI_AuthenticationDescriptor;

    // ID3 Structure
    typedef struct
    {
      CHAR szTAGValidationStr[4];                    // = "TAG" if valid
      CHAR szTitle[31];
      CHAR szArtist[31];
      CHAR szAlbum[31];
      CHAR szYear[5];
      CHAR szComment[30];
```

```
    CHAR cAlbumTrk;
    CHAR cGenreType;
} ID3_TAGDescriptor;
```

As stated above, the pre-encryption process consists of a single encryption method applied to the MP3 content file in order to provide the maximum security to protect the downloaded content 60. The MP3 content file is pre-encrypted using the random 8-byte (64-bit) XOR file key selected by the download server software 312. The XOR file key is also encrypted, using the Blowfish algorithm with the encryption key being the unique ID code of the data storage medium 38. Once the XOR file key is encrypted, the download server software 312 embeds the XOR key in the authentication descriptor for the content player such as the client computer 20, the dedicated playback hardware device or other user-PC application player. The device type bits in the control byte are set to reflect which type of unique ID code was applied as the Blowfish encryption key for the content player. The bit settings are further described above in conjunction with the control byte description.

Fig. 12 illustrates the steps used to create the proper MPI file format for download to the client 26. Block 310 represents the content player software and block 312 represents the download server software.

First, as shown in block 314, the client 26, via the content player software 310, requests content 60 from the download server software 312 of the host site 62. In response, the download server software 312 queries the client 26 for the download destination at block 316. In block 318, the content player software 310 provides the download server software 312 with device type information (i.e. removable storage media, hard drive, CD or other storage device) for the control byte, and if it exists, a download storage path. In block 320, the download server software 312 requests from the content player software 310 for the Blowfish encryption key the unique ID code of the data storage medium 38 associated with the selected download destination. In block 322, the content player software 310 provides the download server software 312 with the unique ID code of the data storage medium 38 for the Blowfish encription key.

In block 324, the OS Type bit is set to reflect operating system type of the MPI file 300. In block 326, the Device Type bit is set to reflect the device type, i.e. the unique ID code type, stored in the authentication descriptor 304. In block 328, the File Type bit is set to reflect MPI file type. In block 330, the encryption/encoder type is set.

In block 332, the download server software 312 creates the random XOR file key. The random XOR file key encryption algorithm is applied to the client-selected MP3 file in block 334 to encrypt the MP3 file. In block 336, the Blowfish encryption key is applied to the random XOR file key using the unique ID code of the data storage medium 38. In block 338, the random XOR file key is placed in the authentication descriptor 304 of the MPI file 300. In block 340, the Blowfish encryption key is applied to the authentication string and in block 342, the encrypted authentication string is placed in the authentication descriptor 304 of the MPI file 300.

In this embodiment, in block 344, a random GIF/AVI advertisement content is selected from a database server associated with or part of the download server, and the length of the GIF/AVI content is determined in block 346. The GIF/AVI content and length are embedded in the authentication descriptor in block 348.

In block 350, the advertising URL hyperlink is associated to the GIF/AVI content, its length is determined and the GIF/AVI hyperlink and length are embedded in the authentication descriptor 304. In block 352, the artist/source URL hyperlink is associated to the MPI file 300, its length determined and the artist/source hyperlink and length are embedded in the authentication descriptor 304.

In block 354, the authentication descriptor (high/low) range and the authentication descriptor size are set in the header 302.

In block 356, the MPI file 300 is created using the following format: Header + Authentication descriptor + Encrypted MP3 content file. In block 358, the MPI file 300 is downloaded to the client 26. In block 360, the content player software 310 stores the MPI file at the selected download destination and stores a content storage path in registry for the content player.

Fig. 13 illustrates the method of and system for playing back the content 60, in this instance the music in the MPI file 300, downloaded in accordance with Fig. 12. In block 362 the client 26 selects the content player software application 310. In block 364, the content player, such as the client computer 20, searches for the content player software 310. If the content player software application 310 is not found, the client 26 is informed of the problem in block 366. If the content player software 310 is found, in block 368, the content player software 310 searches for content 60. If the content 60 is not found, in block 370, the client 26 selects the drive and MPI file to play back. If content 60 is found, in block 372, the content player software 310 determines if more than one MPI file was found. If more than one MPI file was found, then in block 374, the client 26 is queried by the content player software 310 to select the MPI file 300 to be played. In block 376 the client 26 selects the MPI file 300 to play back.

Once the MPI file to play back has been selected, either in block 370, block 372 or block 376, the content player software 310 in block 378 searches for the unique ID code associated with the data storage medium 38. If the unique ID code is not found, the client 26 is informed of the problem in block 366. If the unique ID code is found, in block 380, the XOR file key is decrypted with the Blowfish encryption key using the unique ID code in the Blowfish encryption key. In block 382, the MPI file is decrypted using the XOR file key. In block 384, the MPI file 300 is played and automatically the advertisement 64, advertisement URL hyperlinks for the advertisement 64 and the author, artist and/or source of the MPI content are displayed. All or part of the advertisement 64 or other graphic or text displayed during the playing of the MPI file 300 may also function as a hyperlink to another site associated with the advertisement 64, other graphic or text material.

As is evident from both Figs. 3 and 12, once the client 26 has registered, the client's only step in subsequent visits to the host site 62 may be to select the content 60 desired for download as illustrated at block 162 of Fig. 3 and block 314 of Fig. 12. The client computer 20 may be set up for a default download destination. If not, a second step may be selecting the drive for download as shown in Fig. 6. In instances where the available content 60 is categorized, such as by author,

year or type of content, among other criteria, the selection of the content 60 may be a two step process. The first step is selecting through, for example, a click of the mouse 42A, the category of the content 60 and the second step is selecting through, for example, a click of the mouse 42A, the specific content 60 to be downloaded.

In one embodiment, the host site 62 may provide for the downloading of music from a first page 400 of the host site 62, such as illustrated in Fig. 14. The first page 400 may include graphics 402 as well as textual information 403 associated with the available content, including but not limited to photographs of the content authors or album covers or information about the authors or their works. The graphics 402 or text 403 associated with the content 60 may also function as a hyperlink to further information, graphics or websites associated with the content, such as the content author's personal website. The first page 400 also contains one or more advertisements 64. All or part of the advertisement 64 may also function as a hyperlink associated with the advertiser 54, either to additional information or websites associated with the advertiser or its products.

Also in Fig. 14, the client 26 selects the drive, e.g., the Zip® drive 406, to receive the downloaded music. The client 26 selects a content author among, in this instance, the four content authors 408-414 depicted on the first page 400. When the author is selected, a second page 416 of the host site is displayed as illustrated in Fig. 15, providing a number of specific songs 418 from which the client 26 can select for downloading. As with the first page 400, the second page 416 may include graphics 402 and/or textual information 403 about the authors and/or their works and again the graphics and/or text may also function as a hyperlink. Similar to the first page 400, the second page 416 includes advertisements 64 which optionally may include hyperlinks associated with the advertiser 54.

In one embodiment, the client 20 clicks on one of the songs, e.g., the third song, to start the downloading of the song to the data storage medium 38 of the client computer 20. In an alternative embodiment, the content 60 is selected prior to selecting the download destination. In the alternative embodiment, clicking on the desired content causes a dialog box to be displayed from which the client selects the download destination.

A sponsor or affiliate, such as the advertiser, content owner or content author, associated with the graphics 402 or textual information 403, either on the host site or embedded in the MPI file 300, can be charged in a number of ways including but not limited to, being charged for the initial view of the sponsor's graphic 402 or text 403 on the host site web page, for associating the graphic 402, text 403 and/or hyperlink to the MPI file 300, or for a percentage of the payment for purchases made by traffic created by the hyperlink.

It will be understood by those skilled in the art that individual features or groups of features of the invention can be implemented separate from the rest of the overall system.

Although the invention has been described herein with reference to specific embodiments, many modifications and variations therein will readily occur to those skilled in the art. Accordingly, all such variations and modifications are included within the intended scope of the invention.

CLAIMS

1. A method for protecting content comprising:

obtaining a substantially unique ID code associated with a data storage medium;

encrypting the content by applying a first encryption key to the content;

generating a second encryption key which includes the substantially unique ID code; and

encrypting the first encryption key by applying the second encryption key to the first encryption key.

2. A method for protecting content according to claim 1 further comprising creating a file containing the encrypted content and the encrypted first encryption key.

3. A method for protecting content according to claim 2 further comprising transmitting the file to the data storage medium.

4. A method for protecting content according to claim 3 further comprising using the substantially unique ID code in decrypting the first encryption key and applying the first encryption key to the encrypted content for decrypting the content.

5. A method for protecting content according to claim 2 further comprising:

providing in the file an authentication descriptor; and

including the encrypted first encryption key in the authentication descriptor.

6. A method for protecting content according to claim 5 further comprising providing in the authentication descriptor an encryption type.

7. A method for protecting content according to claim 5 further comprising providing in the authentication descriptor an authentication string for validating the authentication descriptor.

8. A method for protecting content according to claim 5 further comprising providing in the authentication descriptor an encrypted authentication string by applying the second encryption key to an authentication string for validating the authentication descriptor.

9. A method for protecting content according to claim 5 further comprising providing in the authentication descriptor an operating system type, a device type and a file type.

10. A method for protecting content according to claim 2 further comprising providing an embedded advertisement in the file.

11. A method for protecting content according to claim 10 further comprising providing the embedded advertisement in an authentication descriptor of the file.

12. A method for protecting content according to claim 11 further comprising providing in the authentication descriptor the length of the embedded advertisement.

13. A method for protecting content according to claim 2 further comprising providing a first embedded hyperlink in the file.

14. A method for protecting content according to claim 13 further comprising providing the first embedded hyperlink in the authentication descriptor of the file.

15. A method for protecting content according to claim 13 further comprising providing a second embedded hyperlink in the file.

16. A method for protecting content according to claim 13 wherein the first embedded hyperlink is associated with at least one from the group of an advertiser, a content owner and a content author.

17. A method for protecting content according to claim 16 further comprising providing a second embedded hyperlink wherein the second embedded hyperlink is associated with at least one of the group of advertiser, the content owner and the content author.

18. A method for protecting content according to claim 14 further comprising providing in the authentication descriptor the length of the hyperlink.

19. A method for protecting content according to claim 5 further comprising providing in the file a header including file version information and authentication descriptor length.

20. 20. A method for protecting content according to claim 1 wherein the first encryption key is an XOR key.

21. 21. A method for protecting content according to claim 1 wherein the first encryption key is a random key.

22. 22. A method for protecting content according to claim 21 wherein the random key is an XOR key.

23. 23. A method for protecting content according to claim 1 wherein the first encryption key decrypts faster than the second encryption key decrypts.

24. A method for protecting content according to claim 1 wherein the first encryption key is less complex than the second encryption key.

25. A method for protecting patent according to claim 1 wherein the content is music.

26. A system for protecting content comprising:

a substantially unique ID code associated with a data storage medium;

a first encryption key for encrypting content; and

a second encryption key which includes the substantially unique ID code for encrypting the first encryption key by applying the second encryption key to the first encryption key.

27. A system for protecting content according to claim 26 further comprising a file containing the encrypted content and the encrypted first encryption key.

28. A system for protecting content according to claim 27 further comprising a communications network for transmitting the file to the data storage medium.

29. A system for protecting content according to claim 28 wherein the substantially unique ID code is used in decrypting the first encryption key and the first encryption key is applied to the encrypted content for decrypting the content.

30. A system for protecting content according to claim 27 wherein the file further comprises an authentication descriptor which includes the encrypted first encryption key.

31. A system for protecting content according to claim 30 wherein the authentication descriptor further comprises an encryption type.

32. A system for protecting content according to claim 30 wherein the authentication descriptor further comprises an authentication string for validating the authentication descriptor.

33. A system for protecting content according to claim 32 wherein the authentication descriptor further comprises an encrypted authentication string for validating the authentication descriptor.

34. A system for protecting content according to claim 30 wherein the authentication descriptor further comprises an operating system type, a device type and a file type.

35. A system for protecting content according to claim 27 wherein the file further comprises an embedded advertisement.

36. A system for protecting content according to claim 35 wherein the file further comprises an authentication descriptor including the embedded advertisement therein.

37. A system for protecting content according to claim 36 wherein the authentication descriptor further comprises the length of the embedded advertisement.

38. A system for protecting content according to claim 27 wherein the file further comprises a first embedded hyperlink.

39. A system for protecting content according to claim 38 wherein the authentication descriptor further comprises the first embedded hyperlink.

40. A system for protecting content according to claim 38 wherein the file further comprises a second embedded hyperlink.

41. A system for protecting content according to claim 38 wherein the first embedded hyperlink is associated with at least one from the group of an advertiser, a content owner and a content author.

42. A system for protecting content according to claim 41 wherein the file further comprises a second embedded hyperlink and wherein the second embedded hyperlink is associated with at least one of the group of the advertiser, the content owner and the content author.

43. A system for protecting content according to claim 39 wherein the authentication descriptor further comprises the length of the hyperlink.

44. A system for protecting content according to claim 30 wherein the file further comprises a header which includes file version information and authentication descriptor length.

45. A system for protecting content according to claim 26 wherein the first encryption key is an XOR key.

46. A system for protecting content according to claim 26 wherein the first encryption key is a random key.

47. A system for protecting content according to claim 46 wherein the first encryption key is a random XOR key.

48. A system for protecting content according to claim 26 wherein the first encryption key decrypts faster than the second encryption key decrypts.

49. A system for protecting content according to claim 26 wherein the first encryption key is less complex than the second encryption key.

50. A system for protecting content according to claim 26 wherein the content is music.

51. A method of providing content from a host site to a client via a communications network comprising:

obtaining information from the client computer;

prompting the client to select content desired by the client;

responsive to the client selecting the content desired by the client, downloading the selected content from the host site to a download destination; and

charging from at least one in the group of an advertiser, a supplier and an other party for the selected content downloaded;

wherein the only interaction with the client computer required of the client after logging onto the host site for the host site to download the selected content is the client selecting the content.

52. A method of providing content according to claim 51 wherein the client is not charged by the host site for receiving the selected content.

53. A method of providing content from a host site to a client according to claim 51 wherein the step of downloading further comprises downloading the selected content to a data storage medium having a unique ID code.

54. A method of providing content from a host site to a client according to claim 53 further comprising, prior to downloading the selected content, encrypting the selected content with an encryption key that utilizes the unique ID code of the data storage medium so that the selected content can be played back only when the data storage medium to which the selected content was downloaded from the host site is detected by the client computer.

55. A method of providing content from a host site to a client according to claim 53 further comprising, prior to downloading the selected content, encrypting the selected content with an encryption key that utilizes the unique ID code of the data storage medium so that the selected content can be played back only from the data storage medium to which the selected content was downloaded from the host site.

56. A method of providing content from a host site to a client according to claim 51 wherein logging onto the host site consists of the client computer establishing communications with the host site.

57. A method of providing content to a client according to claim 51 wherein logging onto the host site comprises the host site receiving a password from the client computer.

58. A method of providing content to a client according to claim 57, wherein logging onto the host site comprises the client inputting the password into the client computer.

59. A method of providing content from a host site to a client according to claim 51 further comprising downloading an advertisement from the host site that is displayed when the selected content is played back.

60. A method of providing content from a host site to a client according to claim 51 wherein the step of prompting comprises prompting the client to select the content from a displayed list of available content and wherein the only interaction with the client computer required of the client is the client selecting the content from the list of available content.

61. A method of providing content from a host site to a client according to claim 51 wherein the step of prompting further comprises:

prompting the client to select a category of available content;

responsive to the client selecting a category of available content, displaying a list of available content corresponding to the category; and

prompting the client to select the content desired by the client from the list of available content corresponding to the category;

wherein the only interaction with the client computer required of the client is selecting the category of available content from the list of categories of available content and selecting the desired content from the list of available content corresponding to the category.

62. A method of providing content from a host site to a client according to claim 51, wherein the information includes the download destination.

63. A method of providing content from a host site to a client according to claim 51 wherein the content is music.

64. A method of providing content from a host site to a client according to claim 53 wherein the information includes the unique ID code of the data storage medium.

65. A method of providing content from a host site to a client via a communications network comprising:

obtaining information from the client computer;

prompting the client to select content desired by the client;

prompting the client to select a download destination for the content selected by the client;

responsive to the client selecting the content desired by the client and selecting the download destination, downloading the selected content from the host site to the download destination; and

charging from at least one in the group of an advertiser, a supplier and an other party for the selected content downloaded;

wherein the only interaction with the client computer required of the client after logging onto the host site for the host site to download the selected content is the client selecting the content and the download destination.

66. A method of providing content form a host site to a client according to claim 65 wherein the client is not charged by the host site for receiving the selected content.

67. A method of providing content from a host site to a client according to claim 65 wherein the step of downloading further comprises downloading the selected content to a data storage medium having a unique ID code.

68. A method of providing content from a host site to a client according to claim 67 further comprising, prior to downloading the selected content, encrypting the selected content with an encryption key that utilizes the unique ID code of the data storage medium so that the selected content can be played back only when the data storage medium to which the selected content was downloaded from the host site is detected by the client computer.

69. A method of providing content from a host site to a client according to claim 67 further comprising, prior to downloading the selected content, encrypting the selected content with an encryption key that utilizes the unique ID code of the data storage medium so that the selected content can be played back only

from the data storage medium to which the selected content was downloaded from the host site.

70. A method of providing content from a host site to a client according to claim 65 wherein logging onto the host site consists of the client computer establishing communications with the host site.

71. A method of providing content to a client according to claim 65 wherein logging onto the host site comprises the host site receiving a password from the client computer.

72. A method of providing content to a client according to claim 71, wherein logging onto the host site comprises the client inputting the password into the client computer.

73. A method of providing content from a host site to a client according to claim 65 further comprising downloading an advertisement from the host site that is displayed when the selected content is played back.

74. A method of providing content from a host site to a client according to claim 65 wherein the step of prompting comprises prompting the client to select the content from a displayed list of available content and wherein the only interaction with the client computer required of the client is the client selecting the content from the list of available content and selecting the download destination.

75. A method of providing content from a host site to a client according to claim 65 wherein the step of prompting further comprises:

prompting the client to select a category of available content;

responsive to the client selecting a category of available content, displaying a list of available content corresponding to the category; and

prompting the client to select the content desired by the client from the list of available content corresponding to the category;

wherein the only interaction with the client computer required of the client is selecting the category of available content from the list of categories of

available content, selecting the desired content from the list of available content corresponding to the category and selecting the download destination.

76. A method of providing content from a host site to a client according to claim 67 further comprising obtaining information from the client computer and wherein the information includes the unique ID code of the data storage medium.

77. A method of providing content from a host site to a client according to claim 65 wherein the content is music.

78. A system for providing content from a host site to a client via a communications comprising:

a host site having access to content, configured to download the content responsive to a selection of the content by a client, and configured to charge from at least one in the group of an advertiser, a supplier and an other party for the download of the content selected; and

a client computer configured to transmit information to the host site via a communications network and configured to transmit via the communications network the selection of the content by the client based on a single input by the client, subsequent to a logon onto the host site, selecting the content to be downloaded.

79. A system according to claim 78 wherein the host site is configured not to charge the client for downloading the selected content.

80. A system of providing content from a host site to a client according to claim 78 further comprising a data storage medium having a unique ID code for receiving the downloaded content.

81. A system of providing content from a host site to a client according to claim 80 wherein the host site includes an encryption key that utilizes the unique ID code of the data storage medium for encrypting the selected content so that the selected content can be played back only when the data storage medium to which

the selected content was downloaded from the host site is detected by the client computer.

82. A system of providing content from a host site to a client according to claim 80 wherein the host site includes an encryption key that utilizes the unique ID code of the data storage medium for encrypting the selected content so that the selected content can be played back only from the data storage medium to which the selected content was downloaded from the host site.

83. A system of providing content from a host site to a client according to claim 78 further comprising configuring the host site to download an advertisement from the host site that is displayable when the selected content is played back.

84. A system of providing content from a host site to a client according to claim 78 wherein the content is music.

85. A system for providing content from a host site to a client via a communications network comprising:

a host site having access to content, configured to download a list of categories of content, a list of available content in each of the categories and the content responsive to a selection of the content by a client, and configured to charge from at least one in the group of an advertiser, a supplier and an other party for the download of the content selected; and

a client computer configured to transmit information to the host site via a communications network and configured to transmit via the communications network the selection of the content by the client based on only a first input by the client, subsequent to a completion of a logon onto the host site, selecting the category of the content to be downloaded and a second input by the client, subsequent to the completion of the logon onto the host site, selecting the content to be downloaded.

86. A system of providing content from a host site to a client according to claim 85 wherein the host site is configured not to charge the client for downloading the selected content.

87. A system of providing content from a host site to a client according to claim 85, wherein the information includes a download destination.

88. A system of providing content from a host site to a client according to claim 87 wherein the information includes a unique ID code of a data storage medium.

89. A system for providing content from a host site to a client via a communications network subsequent to a client computer logging onto the host site comprising:

a host site having access to content, configured to download the content responsive to a selection of the content by a client, and configured to charge from at least one in the group of an advertiser, a supplier and an other party for the download of the content selected; and

a client computer configured to transmit information to the host site via a communications network and configured to transmit via the communications network the selection of the content by the client based only on a first input by the client, subsequent to a logon onto the host site, selecting the content to be downloaded and a second input by the client, subsequent to a logon onto the host site, selecting download destination for the content.

90. A system of providing content form a host site to a client according to claim 89 wherein the host site is configured not to charge the client for downloading the selected content.

91. A system of providing content from a host site to a client according to claim 89 further comprising a data storage medium having a unique ID code for receiving the downloaded content.

92. A system of providing content from a host site to a client according to claim 89 wherein the host site includes an encryption key that utilizes the unique ID code of the data storage medium for encrypting the selected content so that the selected content can be played back only when the data storage medium to which the selected content was downloaded from the host site is detected by the client computer.

93. A system of providing content from a host site to a client according to claim 89 wherein the host site includes an encryption key that utilizes the unique ID code of the data storage medium for encrypting the selected content so that the selected content can be played back only from the data storage medium to which the selected content was downloaded from the host site.

94. A system of providing content from a host site to a client according to claim 89 further comprising configuring the host site to download an advertisement from the host site that is displayable when the selected content is played back.

95. A method of providing content from a host site to a client according to claim 89 wherein the content is music.

96. A system for providing content from a host site to a client via a communications network comprising:

a host site having access to content, configured to download a list of categories of content, a list of available content in each of the categories and the content responsive to a selection of the content by a client, and configured to charge from at least one in the group of an advertiser, a supplier and an other party for the download of the content selected; and

a client computer configured to transmit information to the host site via a communications network and configured to transmit via the communications network the selection of the content by the client based on only a first input by the client, subsequent to a completion of a logon onto the host site, selecting the category of the content to be downloaded, a second input by the client, subsequent to the

completion of the logon onto the host site, selecting the content to be downloaded and a third input by the client, subsequent to the completion of the logon onto the host site, selecting the download destination for the content.

97. A system of providing content according to claim 96 wherein the host site is configured not to charge the client for downloading the selected content.

98. A system of providing content from a host site to a client according to claim 96, wherein the system is configured for the client computer to provide the information to the host site during the logon, except for the selection of the category, the content and the download destination.

99. A system of providing content from a host site to a client according to claim 96, wherein the system is configured for the client computer to provide the information to the host site subsequent to the logon.

100. A system of providing content from a host site to a client according to claim 99 wherein the information includes a unique ID code of a data storage medium.

101. A system of providing content from a host site to a client according to claim 99 wherein the content is music.

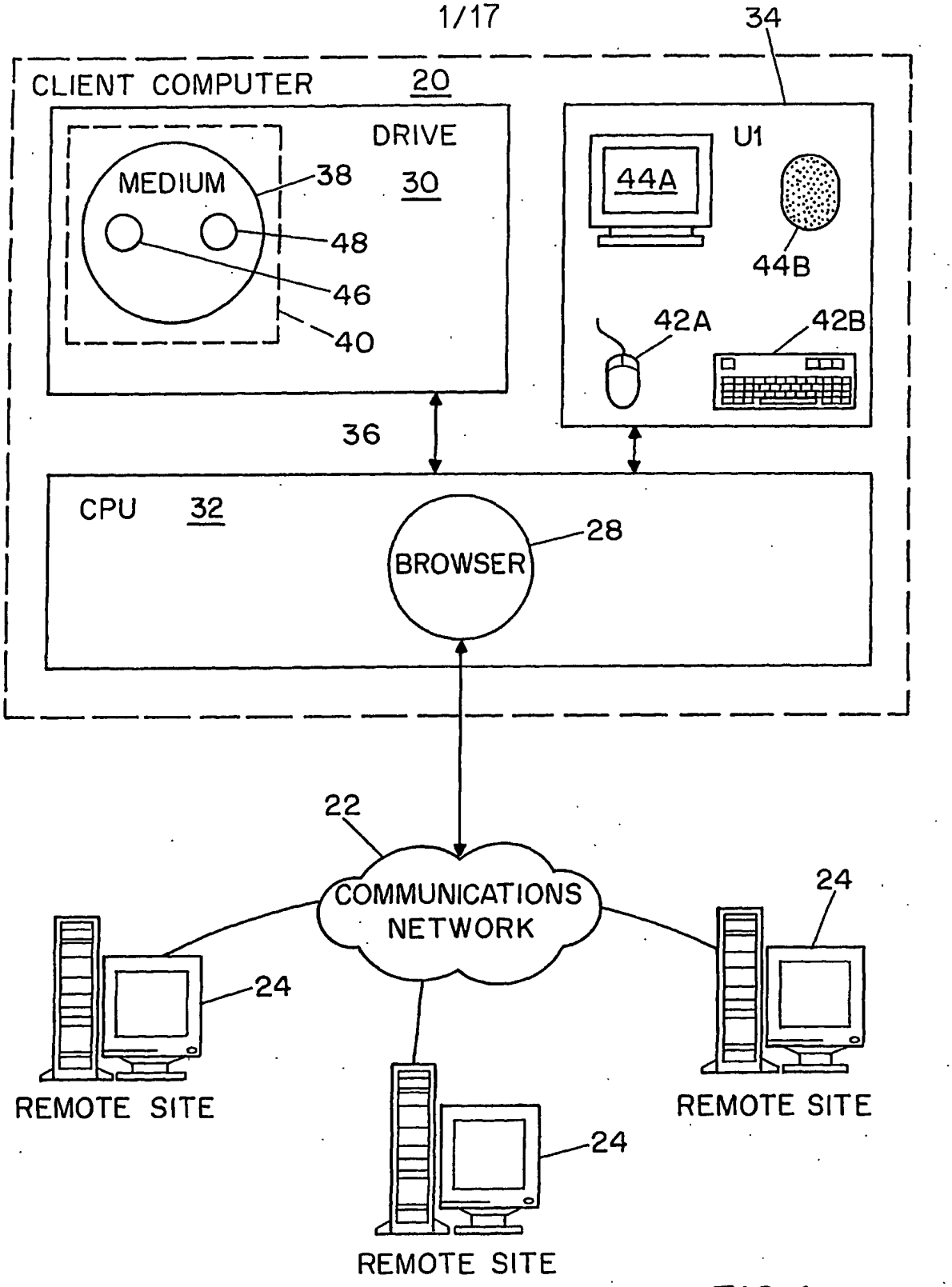

34
CLIENT COMPUTER 20
DRIVE
30
MEDIUM
38
48
46
40
U1
44A
44B
42A
42B
36
CPU 32
BROWSER
28
22
COMMUNICATIONS NETWORK
24
24
24
REMOTE SITE
REMOTE SITE
REMOTE SITE

FIG. 1

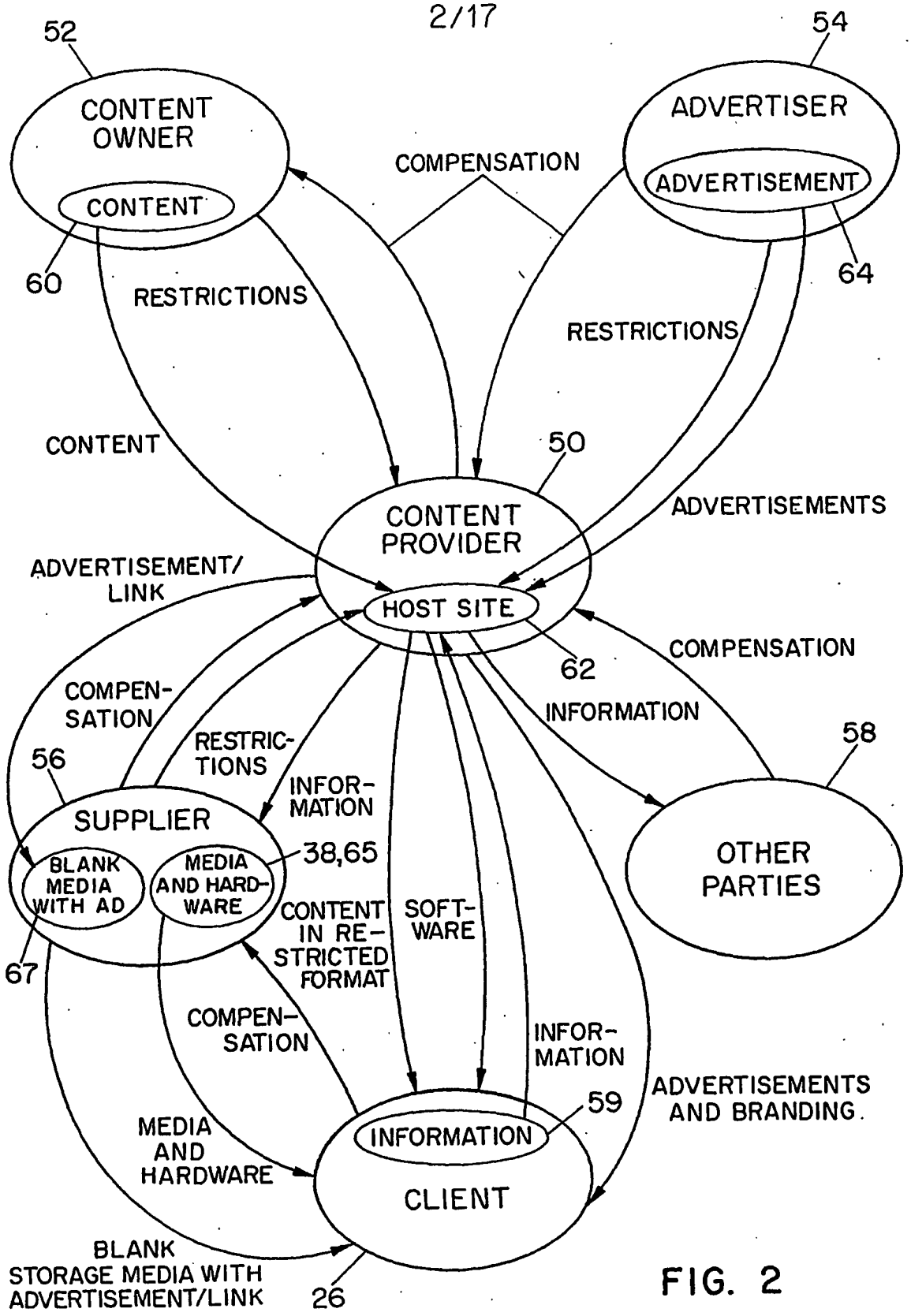

52
CONTENT OWNER
CONTENT
60
54
ADVERTISER
ADVERTISEMENT
64
COMPENSATION
RESTRICTIONS
RESTRICTIONS
CONTENT
50
CONTENT PROVIDER
ADVERTISEMENTS
ADVERTISEMENT/ LINK
HOST SITE
62
COMPENSATION
COMPEN-SATION
INFORMATION
58
RESTRIC-TIONS
56
INFOR-MATION
SUPPLIER
BLANK MEDIA WITH AD
MEDIA AND HARD-WARE
38,65
OTHER PARTIES
CONTENT IN RE-STRICTED FORMAT
SOFT-WARE
67
COMPEN-SATION
INFOR-MATION
ADVERTISEMENTS AND BRANDING
59
INFORMATION
MEDIA AND HARDWARE
CLIENT
BLANK STORAGE MEDIA WITH ADVERTISEMENT/LINK
26

FIG. 2

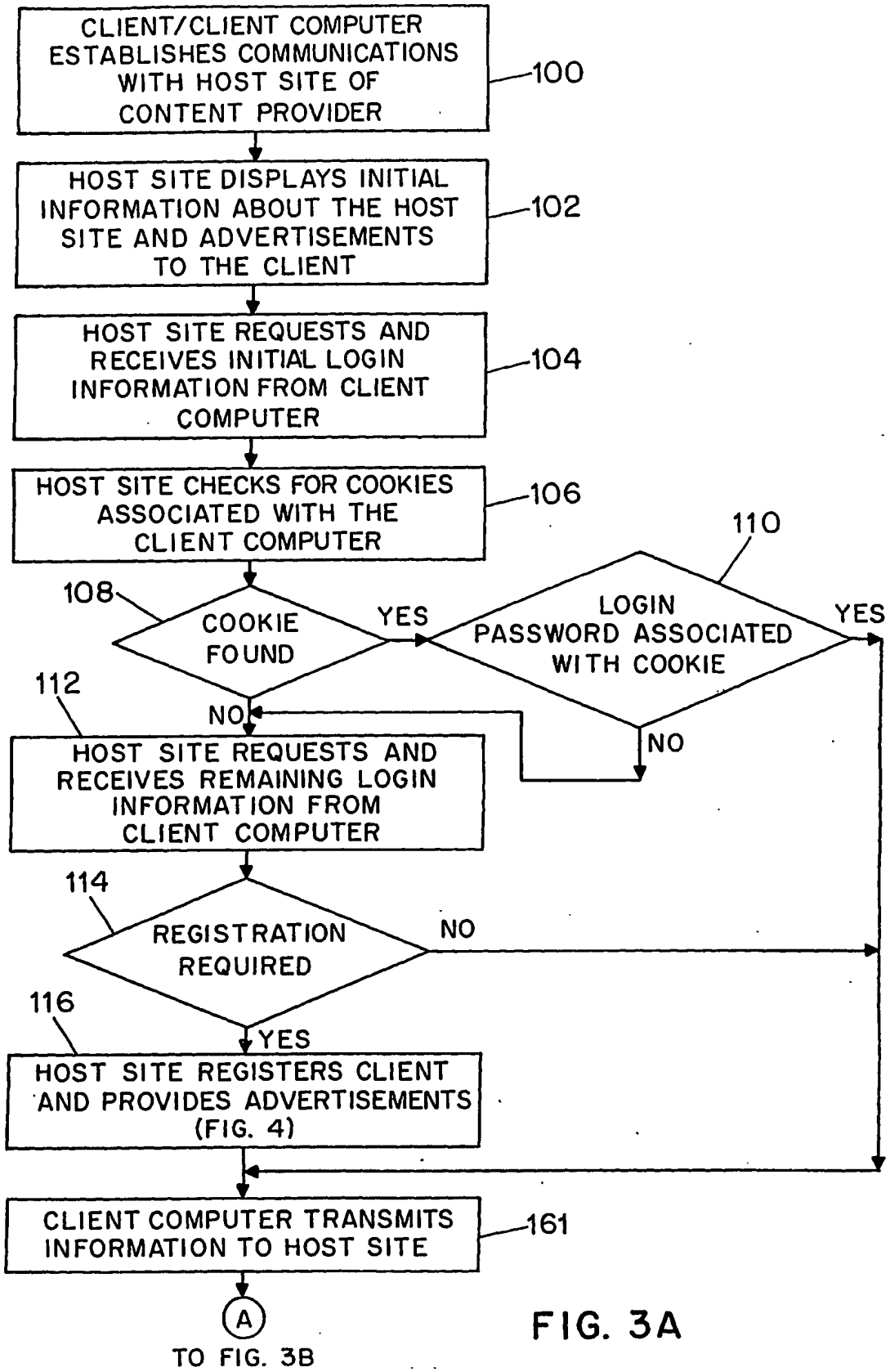

CLIENT/CLIENT COMPUTER ESTABLISHES COMMUNICATIONS WITH HOST SITE OF CONTENT PROVIDER
100
HOST SITE DISPLAYS INITIAL INFORMATION ABOUT THE HOST SITE AND ADVERTISEMENTS TO THE CLIENT
102
HOST SITE REQUESTS AND RECEIVES INITIAL LOGIN INFORMATION FROM CLIENT COMPUTER
104
HOST SITE CHECKS FOR COOKIES ASSOCIATED WITH THE CLIENT COMPUTER
106
108
COOKIE FOUND
YES
110
LOGIN PASSWORD ASSOCIATED WITH COOKIE
YES
NO
NO
112
HOST SITE REQUESTS AND RECEIVES REMAINING LOGIN INFORMATION FROM CLIENT COMPUTER
114
REGISTRATION REQUIRED
NO
YES
116
HOST SITE REGISTERS CLIENT AND PROVIDES ADVERTISEMENTS (FIG. 4)
CLIENT COMPUTER TRANSMITS INFORMATION TO HOST SITE
161
A
TO FIG. 3B

FIG. 3A

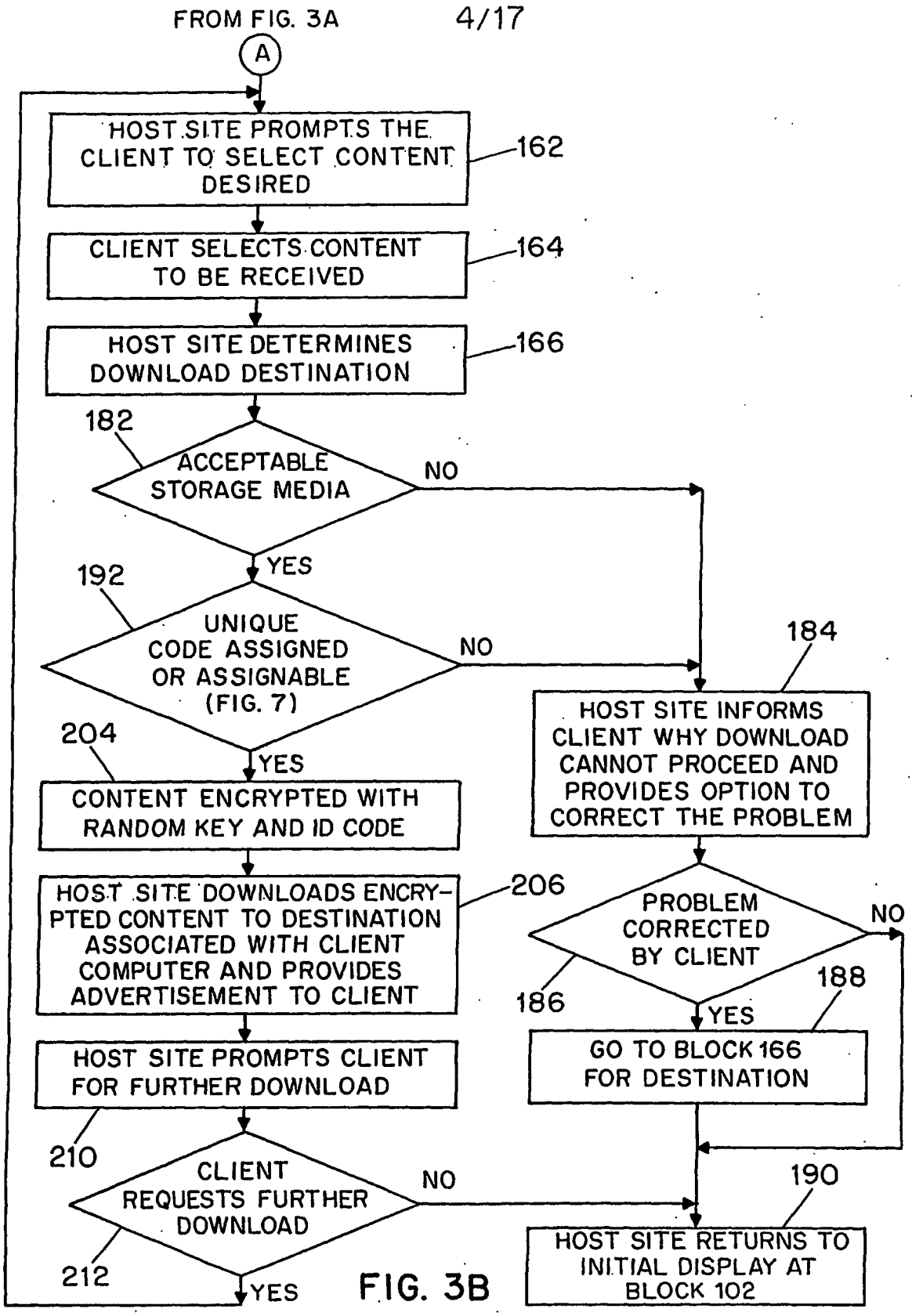

FROM FIG. 3A
A
HOST SITE PROMPTS THE CLIENT TO SELECT CONTENT DESIRED
162
CLIENT SELECTS CONTENT TO BE RECEIVED
164
HOST SITE DETERMINES DOWNLOAD DESTINATION
166
182
ACCEPTABLE STORAGE MEDIA
NO
YES
192
UNIQUE CODE ASSIGNED OR ASSIGNABLE (FIG. 7)
NO
184
YES
204
CONTENT ENCRYPTED WITH RANDOM KEY AND ID CODE
HOST SITE INFORMS CLIENT WHY DOWNLOAD CANNOT PROCEED AND PROVIDES OPTION TO CORRECT THE PROBLEM
206
HOST SITE DOWNLOADS ENCRYPTED CONTENT TO DESTINATION ASSOCIATED WITH CLIENT COMPUTER AND PROVIDES ADVERTISEMENT TO CLIENT
PROBLEM CORRECTED BY CLIENT
NO
186
188
YES
HOST SITE PROMPTS CLIENT FOR FURTHER DOWNLOAD
GO TO BLOCK 166 FOR DESTINATION
210
CLIENT REQUESTS FURTHER DOWNLOAD
NO
190
212
YES
HOST SITE RETURNS TO INITIAL DISPLAY AT BLOCK 102

FIG. 3B

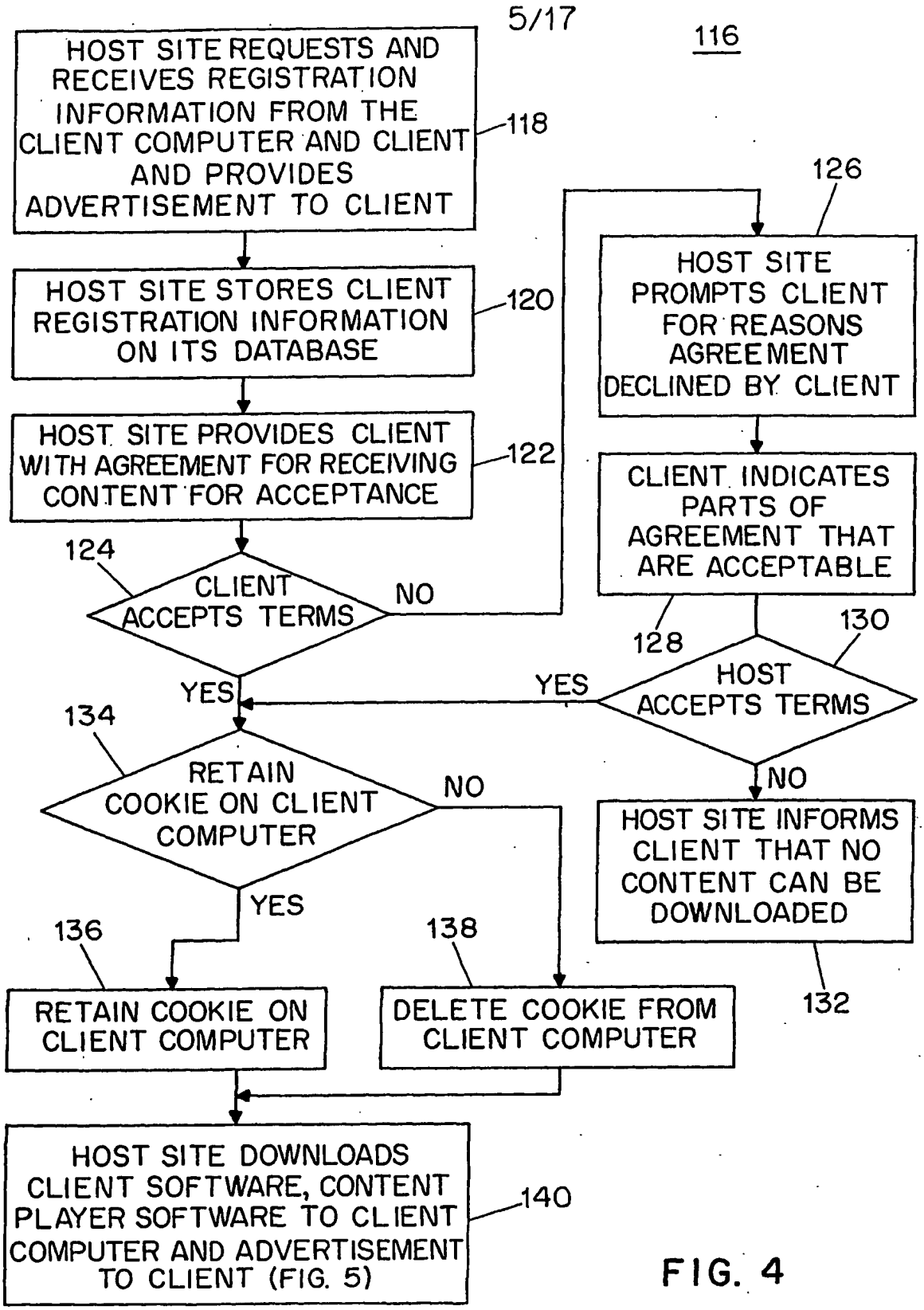

116
HOST SITE REQUESTS AND RECEIVES REGISTRATION INFORMATION FROM THE CLIENT COMPUTER AND CLIENT AND PROVIDES ADVERTISEMENT TO CLIENT
118
HOST SITE STORES CLIENT REGISTRATION INFORMATION ON ITS DATABASE
120
HOST SITE PROVIDES CLIENT WITH AGREEMENT FOR RECEIVING CONTENT FOR ACCEPTANCE
122
124
CLIENT ACCEPTS TERMS
NO
YES
126
HOST SITE PROMPTS CLIENT FOR REASONS AGREEMENT DECLINED BY CLIENT
CLIENT INDICATES PARTS OF AGREEMENT THAT ARE ACCEPTABLE
128
130
HOST ACCEPTS TERMS
YES
NO
134
RETAIN COOKIE ON CLIENT COMPUTER
NO
YES
HOST SITE INFORMS CLIENT THAT NO CONTENT CAN BE DOWNLOADED
132
136
RETAIN COOKIE ON CLIENT COMPUTER
138
DELETE COOKIE FROM CLIENT COMPUTER
HOST SITE DOWNLOADS CLIENT SOFTWARE, CONTENT PLAYER SOFTWARE TO CLIENT COMPUTER AND ADVERTISEMENT TO CLIENT (FIG. 5)
140

FIG. 4

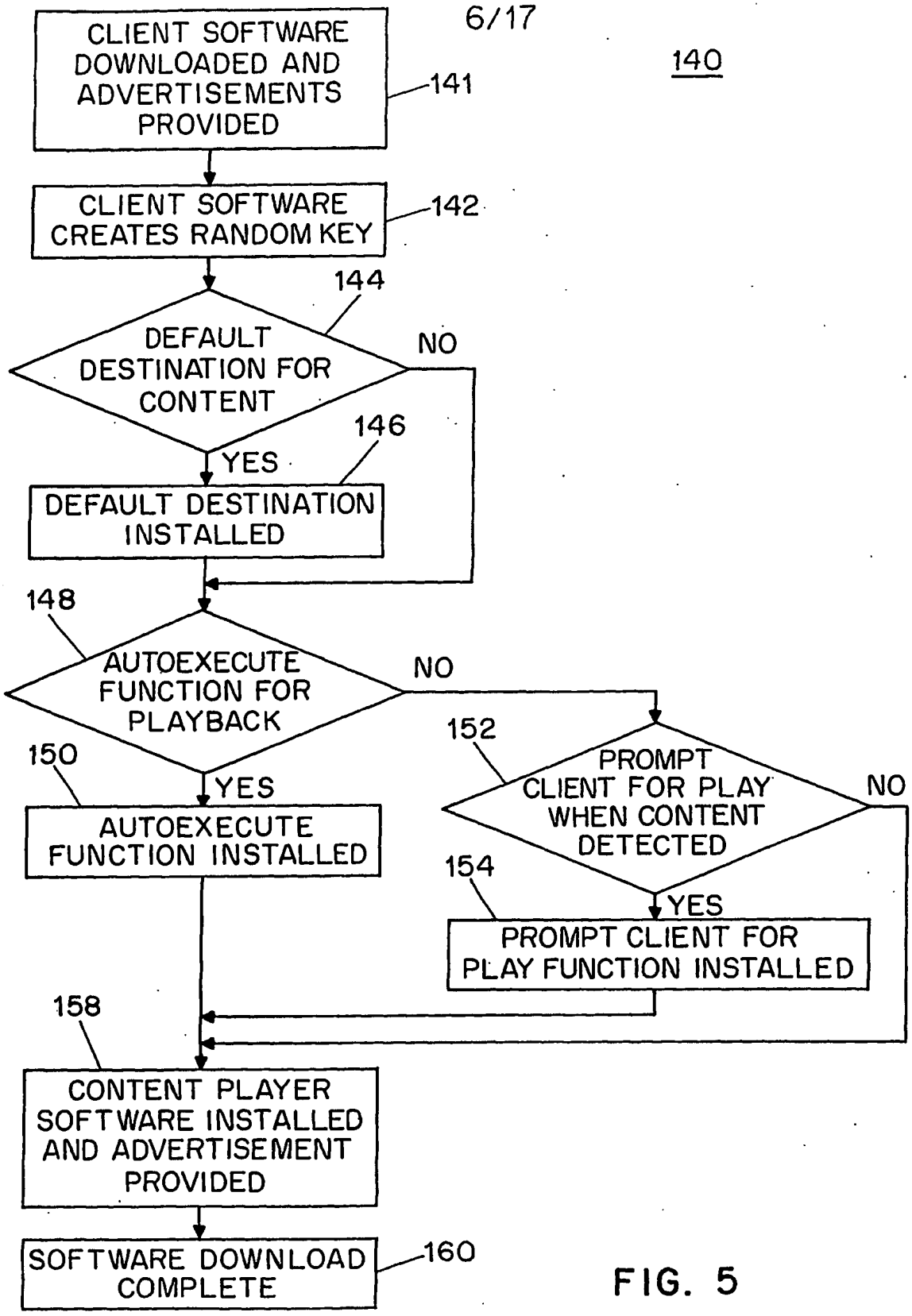

140
CLIENT SOFTWARE DOWNLOADED AND ADVERTISEMENTS PROVIDED
141
CLIENT SOFTWARE CREATES RANDOM KEY
142
144
DEFAULT DESTINATION FOR CONTENT
NO
YES
146
DEFAULT DESTINATION INSTALLED
148
AUTOEXECUTE FUNCTION FOR PLAYBACK
NO
150
YES
AUTOEXECUTE FUNCTION INSTALLED
152
PROMPT CLIENT FOR PLAY WHEN CONTENT DETECTED
NO
154
YES
PROMPT CLIENT FOR PLAY FUNCTION INSTALLED
158
CONTENT PLAYER SOFTWARE INSTALLED AND ADVERTISEMENT PROVIDED
SOFTWARE DOWNLOAD COMPLETE
160

FIG. 5

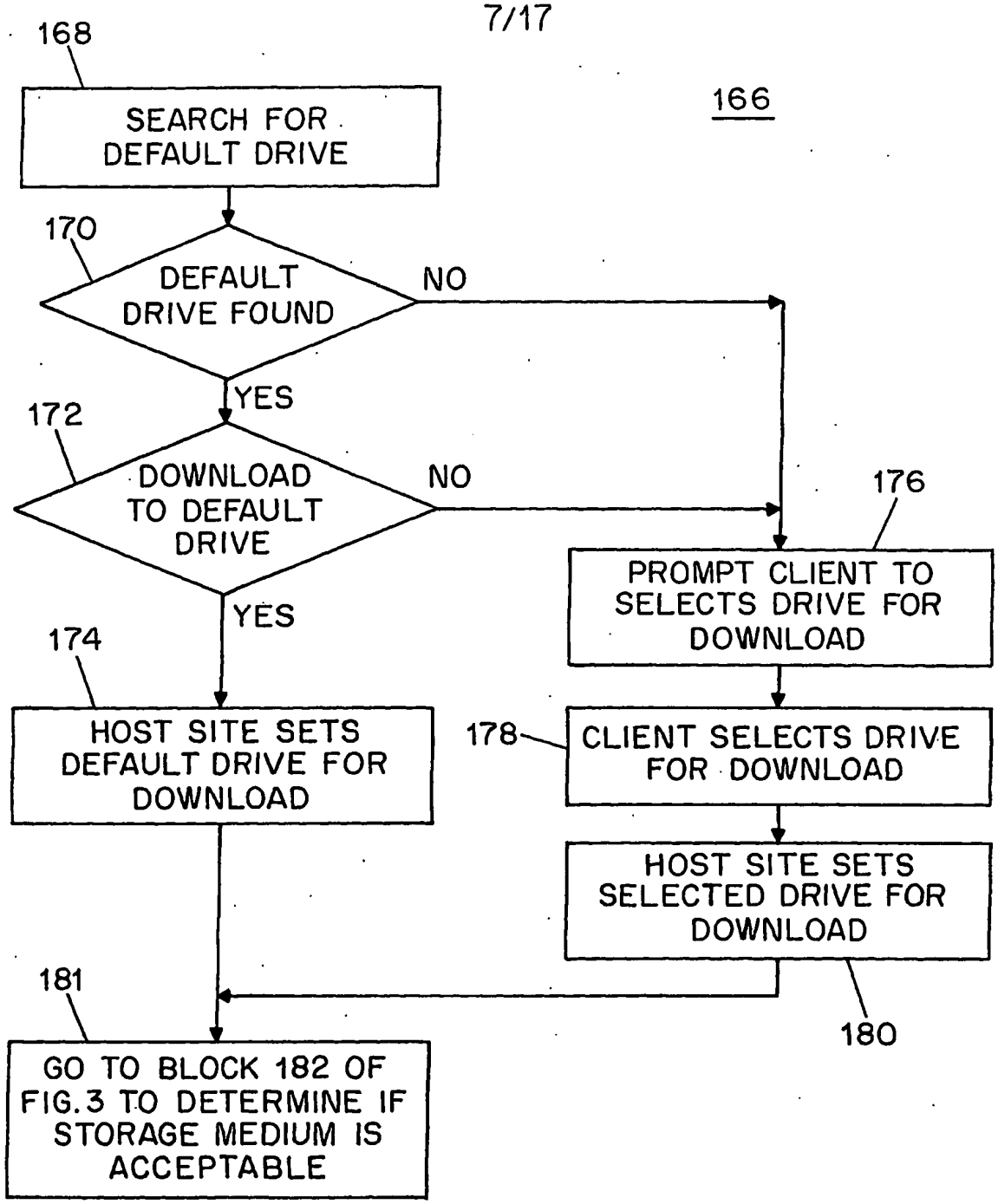

168
SEARCH FOR DEFAULT DRIVE
166
170
DEFAULT DRIVE FOUND
NO
YES
172
DOWNLOAD TO DEFAULT DRIVE
NO
176
PROMPT CLIENT TO SELECTS DRIVE FOR DOWNLOAD
YES
174
HOST SITE SETS DEFAULT DRIVE FOR DOWNLOAD
178
CLIENT SELECTS DRIVE FOR DOWNLOAD
HOST SITE SETS SELECTED DRIVE FOR DOWNLOAD
180
181
GO TO BLOCK 182 OF FIG.3 TO DETERMINE IF STORAGE MEDIUM IS ACCEPTABLE

FIG. 6

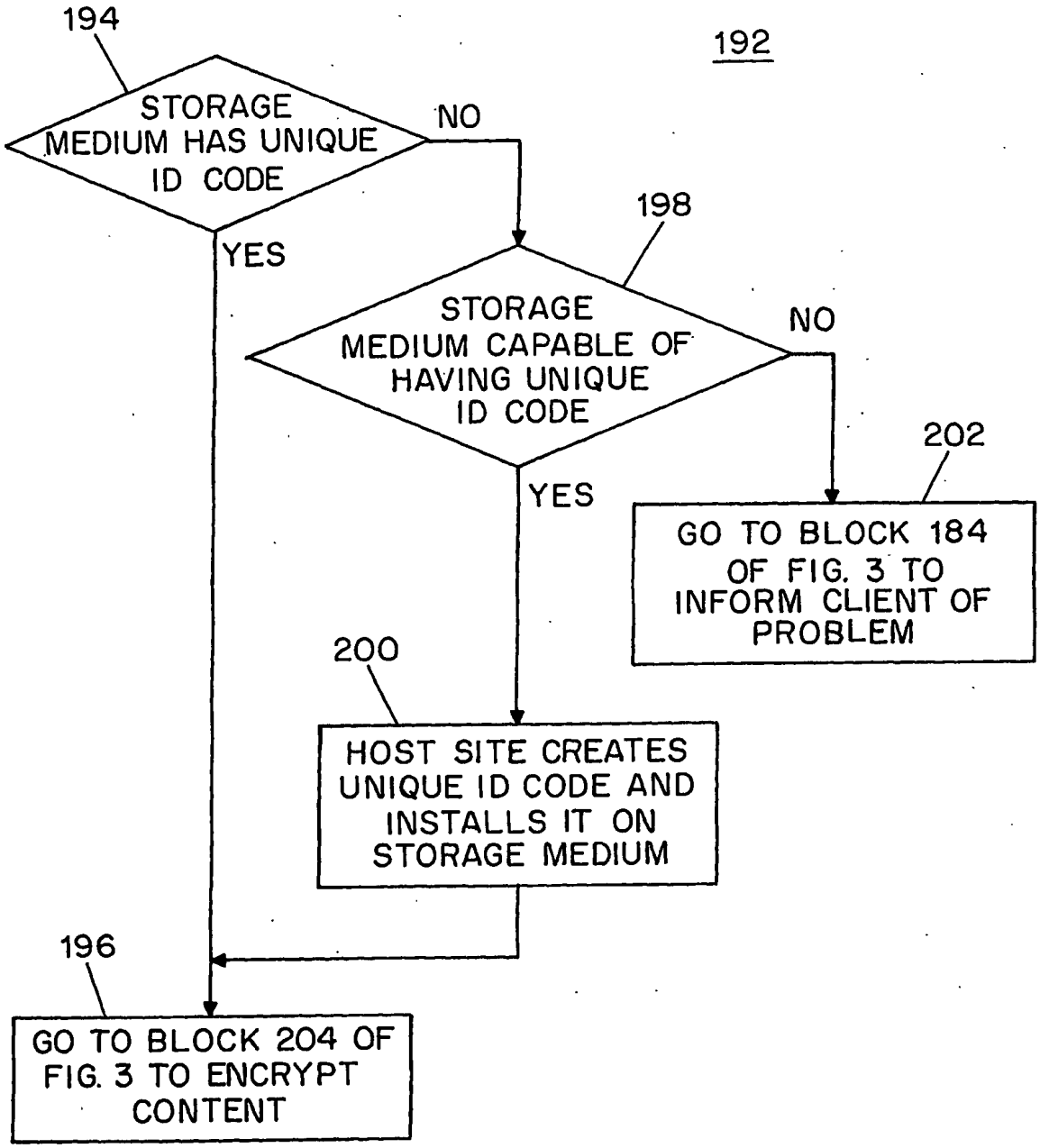

192
194
STORAGE MEDIUM HAS UNIQUE ID CODE
NO
YES
198
STORAGE MEDIUM CAPABLE OF HAVING UNIQUE ID CODE
NO
YES
202
GO TO BLOCK 184 OF FIG. 3 TO INFORM CLIENT OF PROBLEM
200
HOST SITE CREATES UNIQUE ID CODE AND INSTALLS IT ON STORAGE MEDIUM
196
GO TO BLOCK 204 OF FIG. 3 TO ENCRYPT CONTENT

FIG. 7

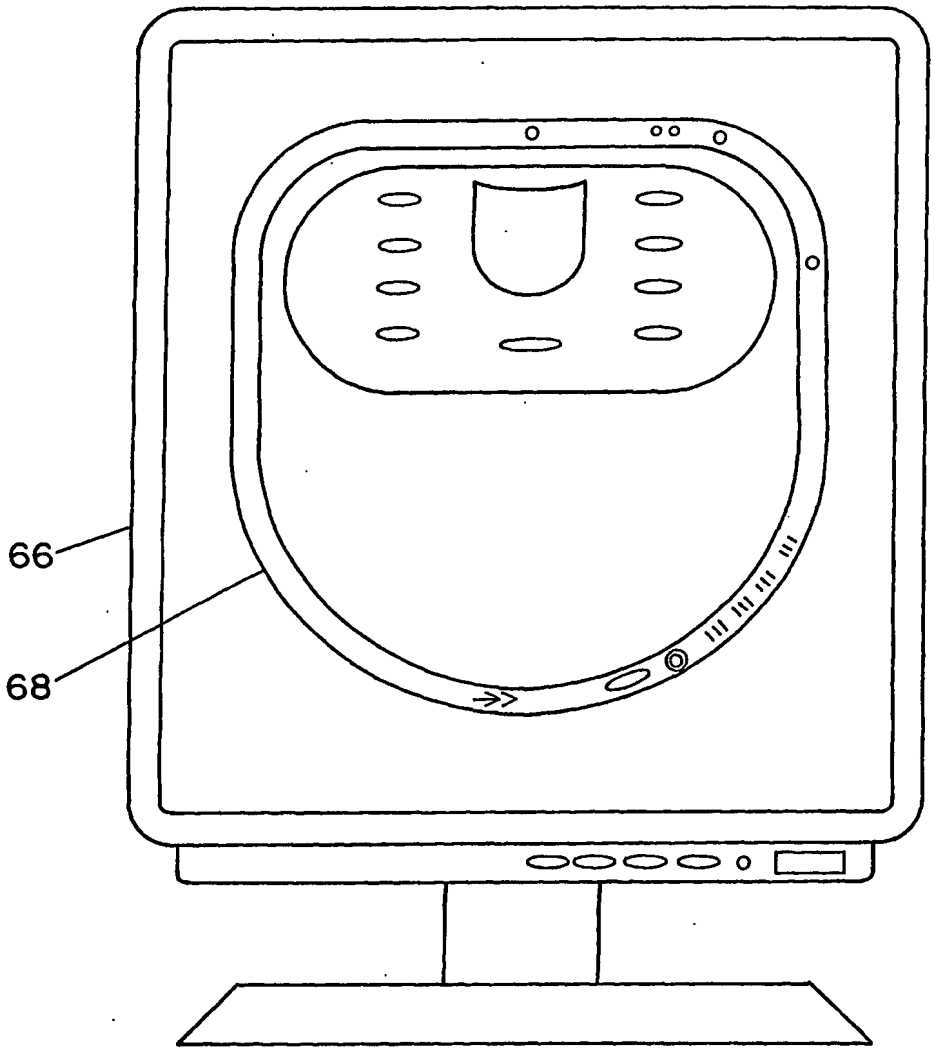


FIG. 8

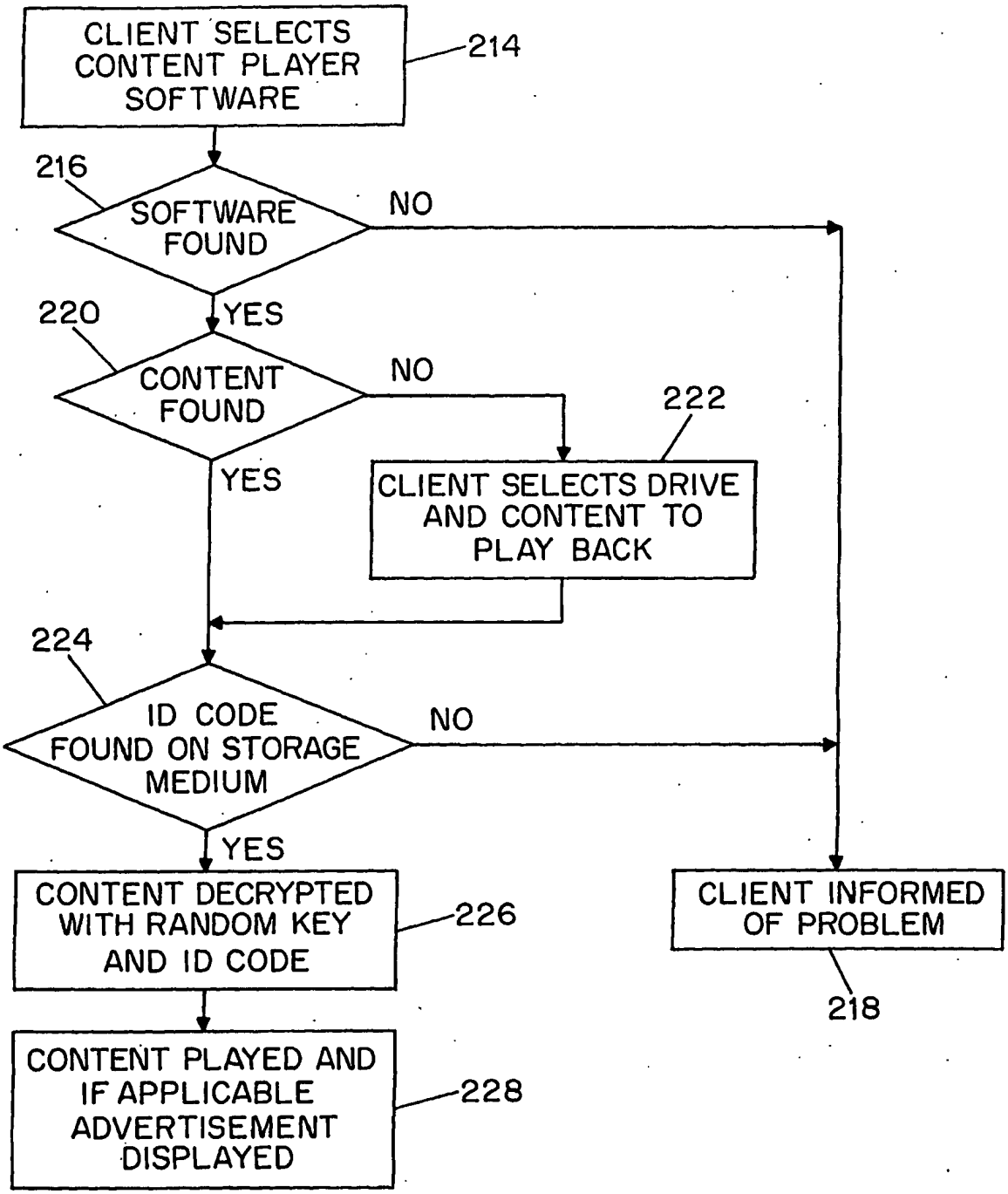

CLIENT SELECTS CONTENT PLAYER SOFTWARE
214
216
SOFTWARE FOUND
NO
YES
220
CONTENT FOUND
NO
222
YES
CLIENT SELECTS DRIVE AND CONTENT TO PLAY BACK
224
ID CODE FOUND ON STORAGE MEDIUM
NO
YES
CONTENT DECRYPTED WITH RANDOM KEY AND ID CODE
226
CLIENT INFORMED OF PROBLEM
218
CONTENT PLAYED AND IF APPLICABLE ADVERTISEMENT DISPLAYED
228

FIG. 9

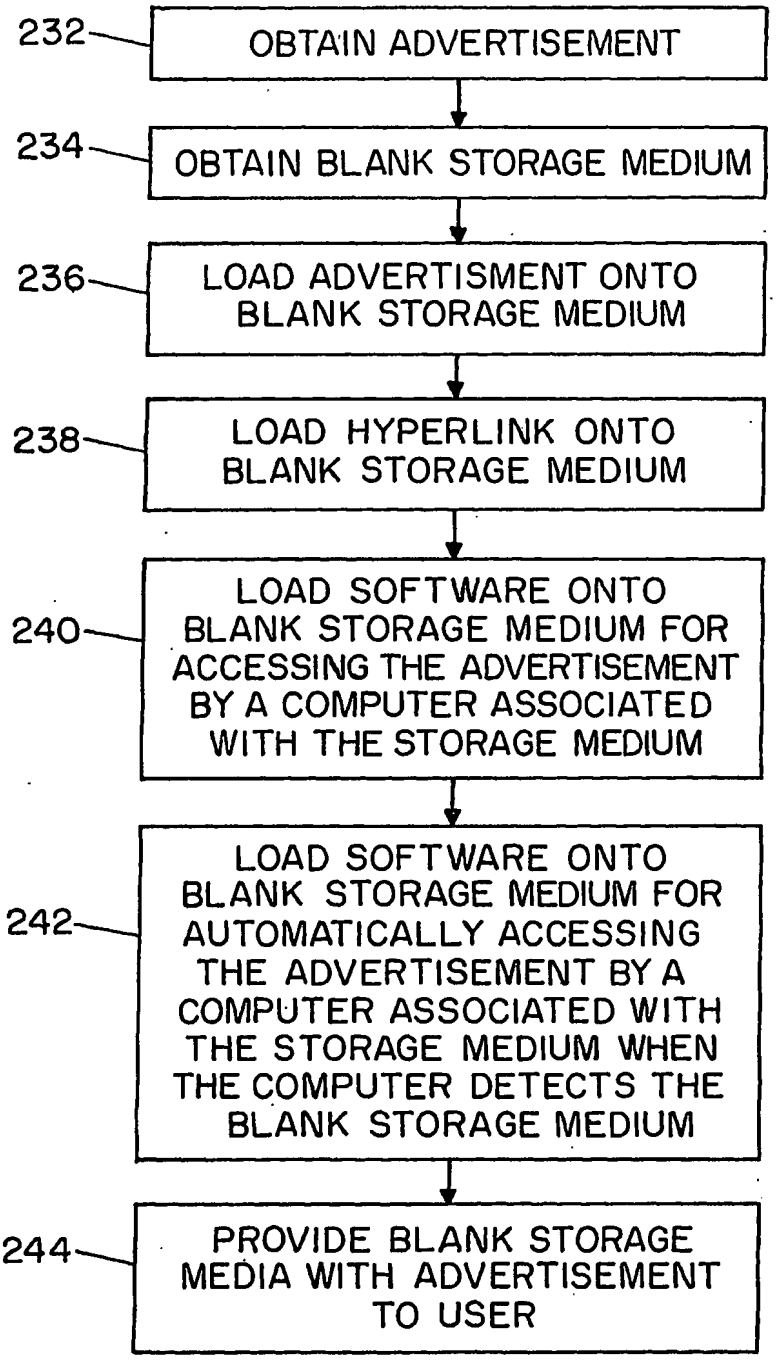

232
OBTAIN ADVERTISEMENT
234
OBTAIN BLANK STORAGE MEDIUM
236
LOAD ADVERTISMENT ONTO BLANK STORAGE MEDIUM
238
LOAD HYPERLINK ONTO BLANK STORAGE MEDIUM
240
LOAD SOFTWARE ONTO BLANK STORAGE MEDIUM FOR ACCESSING THE ADVERTISEMENT BY A COMPUTER ASSOCIATED WITH THE STORAGE MEDIUM
242
LOAD SOFTWARE ONTO BLANK STORAGE MEDIUM FOR AUTOMATICALLY ACCESSING THE ADVERTISEMENT BY A COMPUTER ASSOCIATED WITH THE STORAGE MEDIUM WHEN THE COMPUTER DETECTS THE BLANK STORAGE MEDIUM
244
PROVIDE BLANK STORAGE MEDIA WITH ADVERTISEMENT TO USER

FIG. 10

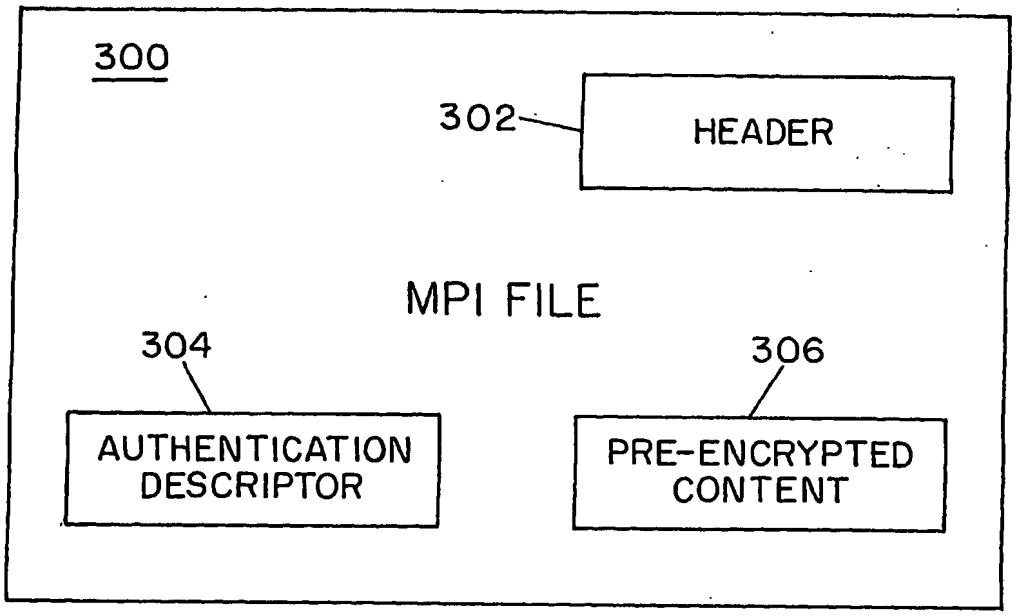

300
302
HEADER
MPI FILE
304
306
AUTHENTICATION DESCRIPTOR
PRE-ENCRYPTED CONTENT

FIG. 11

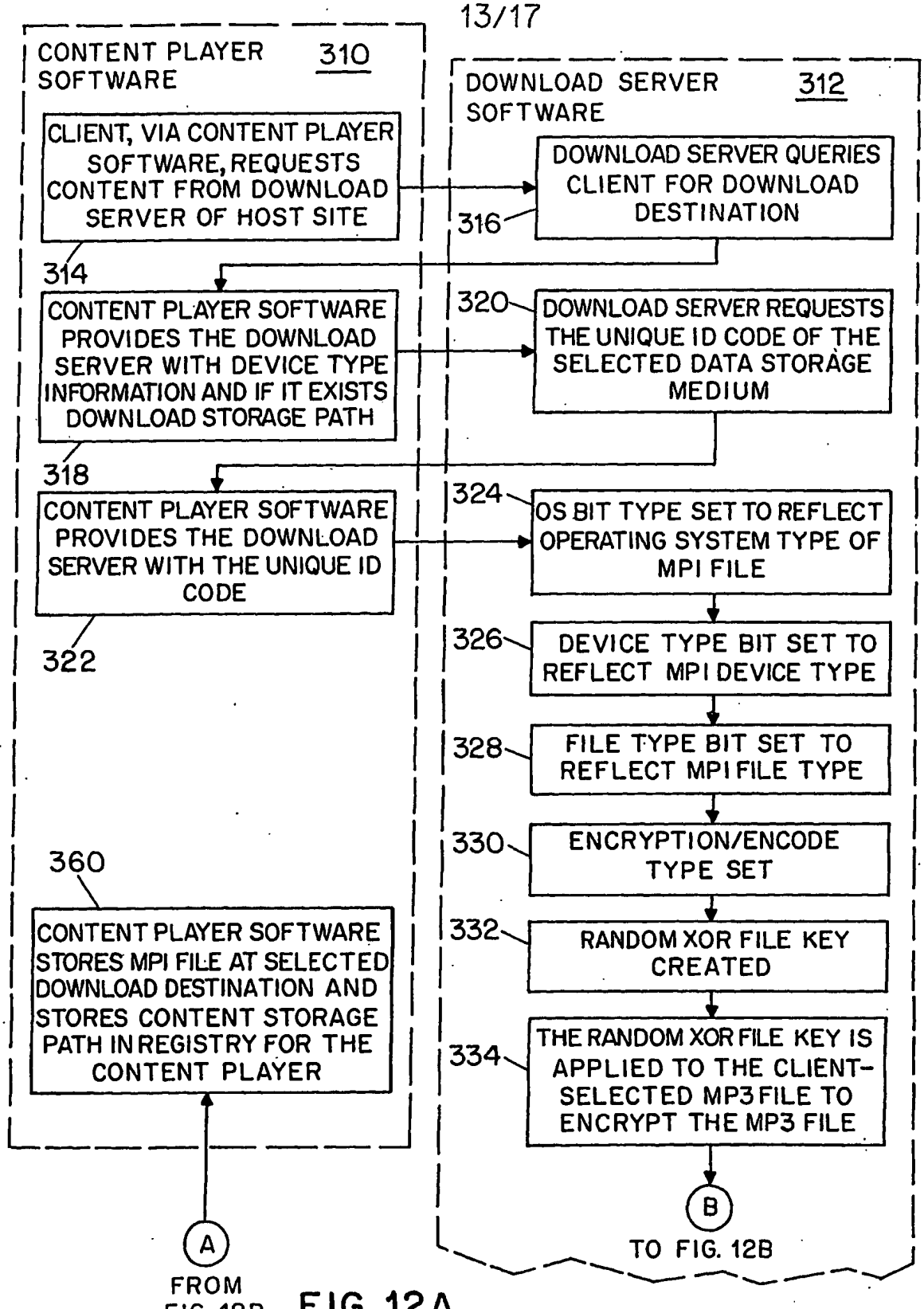

CONTENT PLAYER SOFTWARE 310
CLIENT, VIA CONTENT PLAYER SOFTWARE, REQUESTS CONTENT FROM DOWNLOAD SERVER OF HOST SITE
314
CONTENT PLAYER SOFTWARE PROVIDES THE DOWNLOAD SERVER WITH DEVICE TYPE INFORMATION AND IF IT EXISTS DOWNLOAD STORAGE PATH
318
CONTENT PLAYER SOFTWARE PROVIDES THE DOWNLOAD SERVER WITH THE UNIQUE ID CODE
322
360
CONTENT PLAYER SOFTWARE STORES MPI FILE AT SELECTED DOWNLOAD DESTINATION AND STORES CONTENT STORAGE PATH IN REGISTRY FOR THE CONTENT PLAYER
A
FROM FIG. 12B
DOWNLOAD SERVER SOFTWARE 312
DOWNLOAD SERVER QUERIES CLIENT FOR DOWNLOAD DESTINATION
316
320
DOWNLOAD SERVER REQUESTS THE UNIQUE ID CODE OF THE SELECTED DATA STORAGE MEDIUM
324
OS BIT TYPE SET TO REFLECT OPERATING SYSTEM TYPE OF MPI FILE
326
DEVICE TYPE BIT SET TO REFLECT MPI DEVICE TYPE
328
FILE TYPE BIT SET TO REFLECT MPI FILE TYPE
330
ENCRYPTION/ENCODE TYPE SET
332
RANDOM XOR FILE KEY CREATED
334
THE RANDOM XOR FILE KEY IS APPLIED TO THE CLIENT-SELECTED MP3 FILE TO ENCRYPT THE MP3 FILE
B
TO FIG. 12B

FIG. 12A

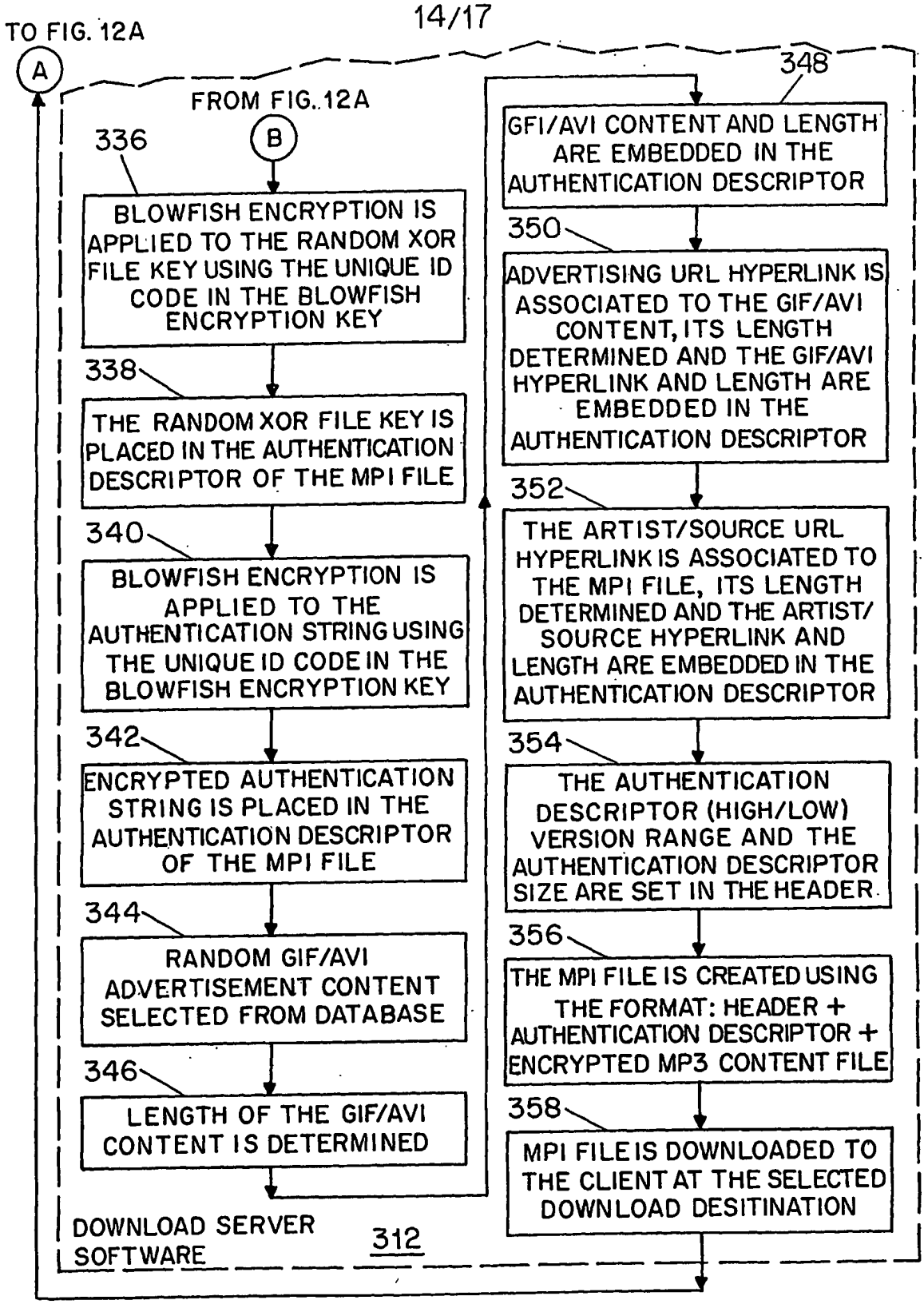

TO FIG. 12A
A
FROM FIG. 12A
B
336
BLOWFISH ENCRYPTION IS APPLIED TO THE RANDOM XOR FILE KEY USING THE UNIQUE ID CODE IN THE BLOWFISH ENCRYPTION KEY
338
THE RANDOM XOR FILE KEY IS PLACED IN THE AUTHENTICATION DESCRIPTOR OF THE MPI FILE
340
BLOWFISH ENCRYPTION IS APPLIED TO THE AUTHENTICATION STRING USING THE UNIQUE ID CODE IN THE BLOWFISH ENCRYPTION KEY
342
ENCRYPTED AUTHENTICATION STRING IS PLACED IN THE AUTHENTICATION DESCRIPTOR OF THE MPI FILE
344
RANDOM GIF/AVI ADVERTISEMENT CONTENT SELECTED FROM DATABASE
346
LENGTH OF THE GIF/AVI CONTENT IS DETERMINED
348
GFI/AVI CONTENT AND LENGTH ARE EMBEDDED IN THE AUTHENTICATION DESCRIPTOR
350
ADVERTISING URL HYPERLINK IS ASSOCIATED TO THE GIF/AVI CONTENT, ITS LENGTH DETERMINED AND THE GIF/AVI HYPERLINK AND LENGTH ARE EMBEDDED IN THE AUTHENTICATION DESCRIPTOR
352
THE ARTIST/SOURCE URL HYPERLINK IS ASSOCIATED TO THE MPI FILE, ITS LENGTH DETERMINED AND THE ARTIST/ SOURCE HYPERLINK AND LENGTH ARE EMBEDDED IN THE AUTHENTICATION DESCRIPTOR
354
THE AUTHENTICATION DESCRIPTOR (HIGH/LOW) VERSION RANGE AND THE AUTHENTICATION DESCRIPTOR SIZE ARE SET IN THE HEADER
356
THE MPI FILE IS CREATED USING THE FORMAT: HEADER + AUTHENTICATION DESCRIPTOR + ENCRYPTED MP3 CONTENT FILE
358
MPI FILE IS DOWNLOADED TO THE CLIENT AT THE SELECTED DOWNLOAD DESITINATION
DOWNLOAD SERVER SOFTWARE
312

FIG. 12B

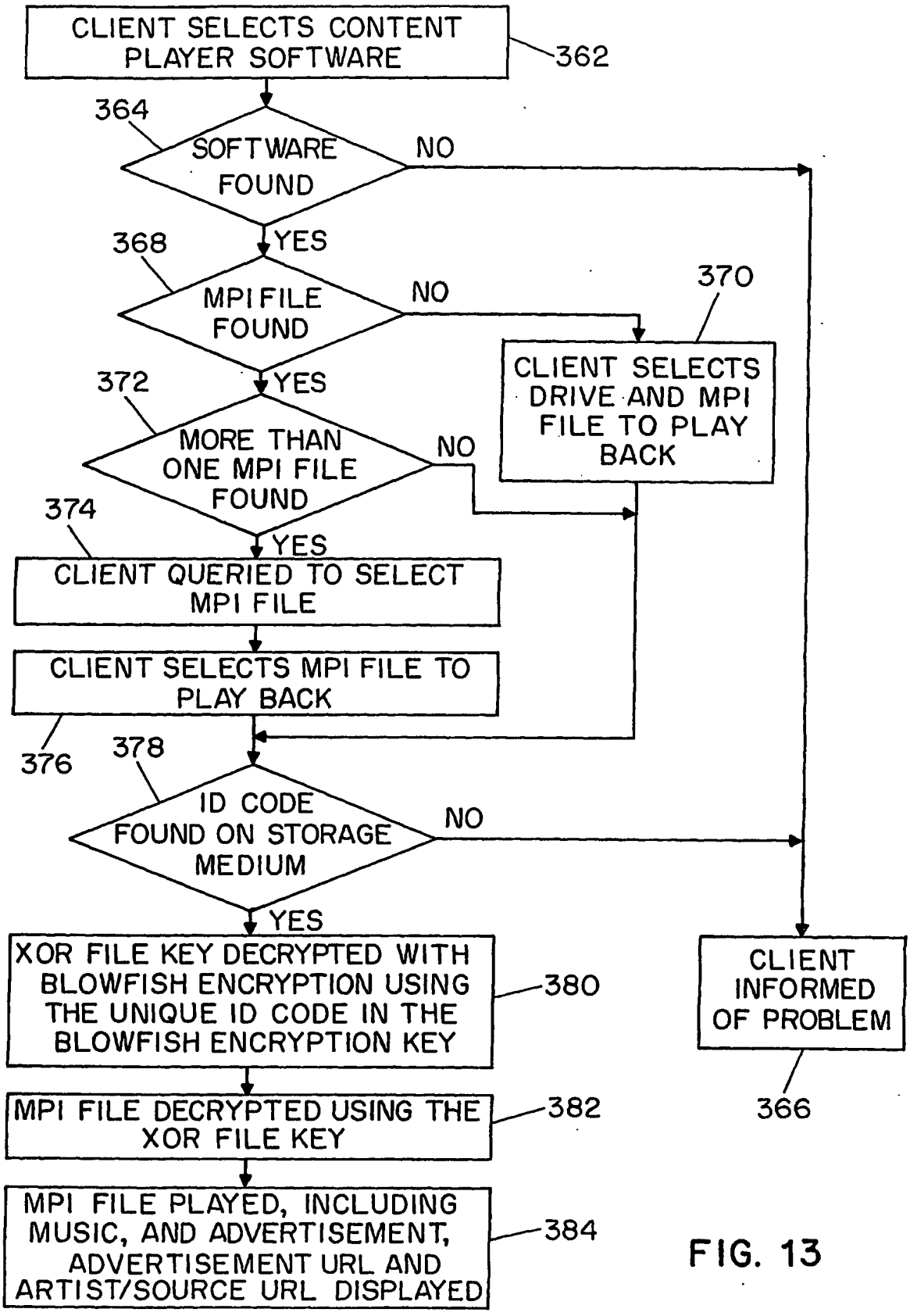

CLIENT SELECTS CONTENT PLAYER SOFTWARE
362
364
SOFTWARE FOUND
NO
YES
368
MPI FILE FOUND
NO
370
CLIENT SELECTS DRIVE AND MPI FILE TO PLAY BACK
YES
372
MORE THAN ONE MPI FILE FOUND
NO
374
YES
CLIENT QUERIED TO SELECT MPI FILE
CLIENT SELECTS MPI FILE TO PLAY BACK
376
378
ID CODE FOUND ON STORAGE MEDIUM
NO
YES
XOR FILE KEY DECRYPTED WITH BLOWFISH ENCRYPTION USING THE UNIQUE ID CODE IN THE BLOWFISH ENCRYPTION KEY
380
CLIENT INFORMED OF PROBLEM
366
MPI FILE DECRYPTED USING THE XOR FILE KEY
382
MPI FILE PLAYED, INCLUDING MUSIC, AND ADVERTISEMENT, ADVERTISEMENT URL AND ARTIST/SOURCE URL DISPLAYED
384

FIG. 13

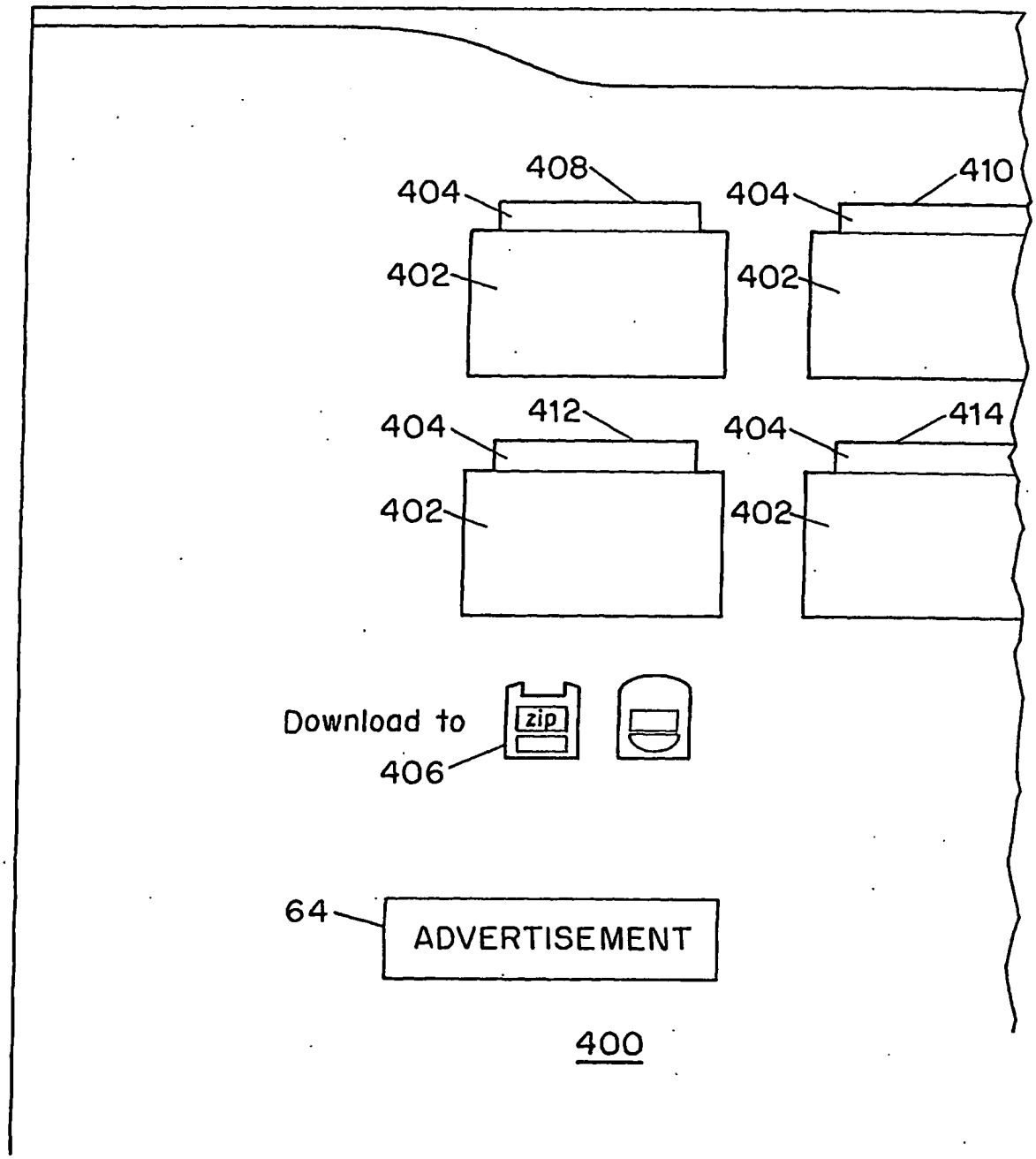

408
404
410
404
402
402
412
404
414
404
402
402
Download to
zip
406
64
ADVERTISEMENT
400

FIG. 14

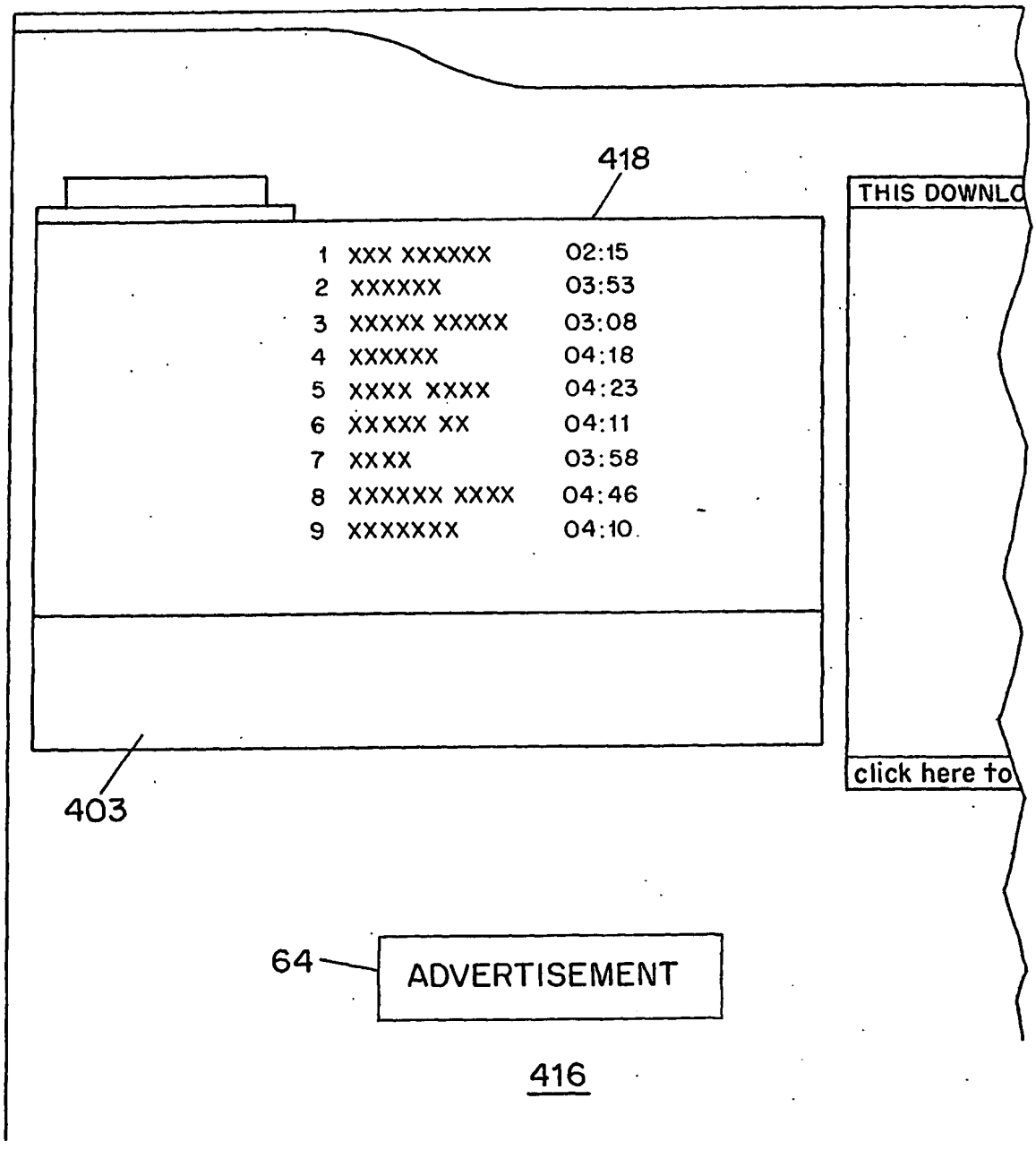

418
THIS DOWNLO
1 XXX XXXXXX 02:15
2 XXXXXX 03:53
3 XXXXX XXXXX 03:08
4 XXXXXX 04:18
5 XXXX XXXX 04:23
6 XXXXX XX 04:11
7 XXXX 03:58
8 XXXXXX XXXX 04:46
9 XXXXXXX 04:10
click here to
403
64
ADVERTISEMENT
416

FIG. 15